Symantec™ Client Security Client Guide

Symantec™ Client Security Client Guide

Documentation version 3.0

Copyright Notice

Trademarks

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/ function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support Program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Contents

Chapter 3 Protecting your computer from viruses and security risks

Chapter 4 What to do if a virus or security risk is found

Index

Section 1

Symantec AntiVirus

Chapter 1

Introducing Symantec AntiVirus

This chapter includes the following topics:

About Symantec AntiVirus

You can install Symantec AntiVirus™ virus and security risk protection as either a stand-alone or an administrator-managed installation. A stand-alone installation means that your Symantec AntiVirus software is not managed by a network administrator.

If you manage your own computer, it must be one of the following types:

- A stand-alone computer that is not connected to a network, such as a home computer or a laptop stand-alone, with a Symantec AntiVirus installation that uses either the default option settings or administrator-preset options settings
- A remote computer that connects to your corporate network that must meet security requirements before connecting

The default settings for Symantec AntiVirus provide virus and security risk protection for your computer. However, you may want to adjust them to suit your company's needs, to optimize system performance, and to disable options that do not apply.

If your installation is managed by your administrator, some options may be locked or unavailable, or may not appear at all, depending upon your administrator's security policy. Your administrator runs scans on your computer and can set up scheduled scans.

Your administrator can advise you as to what tasks you should perform by using Symantec AntiVirus.

Note: Options that display a padlock icon are not available because they have been locked by your administrator. You cannot change these options unless the administrator unlocks them.

About updating stand-alone computers

Stand-alone computers may be connected to the Internet. In Symantec AntiVirus documentation, the term stand-alone takes on an added dimension. Stand-alone computers are not connected to a server; thus they do not receive virus and security risk definitions updates from the server, and cannot be managed by the Symantec System Center administrator program.

If you installed Symantec AntiVirus on a stand-alone computer, you are responsible for updating the virus and security risk definitions. New definitions files are available several times each month from Symantec. You will be alerted when definitions files need replacing.

You can update the virus and security risk definitions files with LiveUpdate™. LiveUpdate retrieves the new definitions files from a Symantec site, and then replaces the old definitions files in the Symantec AntiVirus directory. A modem or Internet connection is required.

See "Updating protection immediately with LiveUpdate" on page 39.

About remote computers that connect to a corporate network

Remote computers that connect to a corporate network can receive virus and security risk definitions, and can be managed by the Symantec System Center administrator program.

System administrators may require remote computers that connect to a corporate network to meet some security requirements. For example, the computer may have to run Symantec AntiVirus with the most up-to-date virus and security risk definitions before it can connect to the network. The computer may be denied access to the network until it meets the security requirements.

About viruses

A *virus* is a computer program that attaches a copy of itself to another computer program or document when it runs. Whenever the infected program runs or a user opens a document containing a macro virus, the attached virus program activates and attaches itself to other programs and documents.

Viruses generally deliver a payload, such as displaying a message on a particular date. Some viruses specifically damage data by corrupting programs, deleting files, or reformatting disks.

A *worm* is a special type of virus that replicates itself from one computer to another and can use memory. Worms generally exist inside other files, such as Microsoft® Word or Excel documents. A worm may release a document that already has the worm macro inside of it.

A *blended threat* combines the characteristics of viruses, worms, Trojan horses, and malicious code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. Blended threats use multiple methods and techniques to propagate and attack, and cause widespread damage throughout a network.

In the context of Symantec AntiVirus, the term virus is used to cover all threats that work in a virus-like manner. Symantec AntiVirus can detect, delete, and quarantine viruses, and repair the side effects of viruses.

A *security risk* is a known program, in a category such as adware or spyware, that may or may not present a risk to the security of a computer. Symantec AntiVirus can detect, quarantine, and repair the side effects of risks in these security risk categories.

See “About security risks” on page 18.

How viruses spread

Viruses can spread through any network, modem, or magnetic medium. Most boot viruses can only spread by way of floppy disks. Multipartite viruses are especially elusive because they can travel as file viruses, infect boot sectors, and be transmitted through floppy disks.

The growth of LAN, Internet, and global email connectivity has accelerated the rate at which viruses can spread. A localized virus outbreak can quickly spread to another part of a company or the world when infected files are sent through email. The primary threat of virus infection comes from files that are shared, and then opened and used.

Virus types

Viruses are classified by what they infect and how they attempt to evade detection. The basic virus types are defined by the area of the computer that they infect, such as boot viruses, file viruses, and macro viruses.

Other types of destructive code include worms and Trojan horses. These types of destructive code are different than viruses because they don't replicate.

Boot viruses

Boot viruses insert instructions into the boot sectors of floppy disks, or the boot sector or master boot record (partition sector) of a hard disk. Boot viruses are some of the most successful viruses.

When the computer starts from an infected floppy disk, the virus infects the hard disk and loads its code into memory. The floppy disk does not have to be a startup disk for the virus to spread. The virus remains memory-resident and infects any floppy disks that are accessed. A floppy disk or hard disk with an infected boot sector won't infect any files unless the virus is also multipartite. A true boot virus can't spread to a server or over the network.

See "About the master boot record" on page 17.

File viruses

File viruses attach to executable files such as .com, .exe, and .dll files by inserting instructions into the execution sequence. When the infected file runs, the inserted instructions execute the virus code. After the code finishes executing, the file continues with its normal execution sequence. This happens so quickly that you're not aware that the virus executed.

There are three subclassifications of file viruses:

- Memory-resident: Stay in memory as terminate-stay-resident (TSR) programs and typically infect all executed files.
- Direct action: Execute, infect other files, and unload.
- Companion: Associate themselves with executable files without modifying them. For example, the virus might create a companion file, Word.com, and attach it to the Word.exe file. When the Word program opens, the infected Word.com file executes, performs the virus activities, and then executes the Word.exe file.

The damage that is caused by file viruses ranges from irritating, such as displaying screen messages, to data destroying.

Macro viruses

Unlike other viruses, macro viruses do not infect program files; they infect documents. Common targets for many macro viruses are word processors such as Microsoft Word and Lotus AmiPro®, and spreadsheets like Microsoft Excel.

Word uses macros to perform actions such as formatting text and opening or closing a document. Macro viruses can modify macros that are defined by the Word application to perform malicious actions such as overwriting or redefining default definitions in Word.

The damage that is caused by macro viruses can range from inserting unwanted text into documents to significantly reducing the functionality of a computer.

Macro viruses that infect Word commonly target the macros that are associated with the Normal.dot template. This template is global, so all of your Word files can be infected.

About the master boot record

The master boot record is contained on the first sector of a hard drive. Part of the process of starting a computer includes giving control to the hard disk. Also, a program is located in the first sector of the hard disk that enables the operating system to load into random access memory (RAM).

Boot viruses can damage the master boot record by moving, overwriting, or deleting it. For example, the Monkey virus moves the master boot record to the hard drive's third sector, and then places its own code in the first sector. Moving the master boot record makes starting from the hard drive impossible.

See "Boot viruses" on page 16.

About security risks

Security risks are classified by the behavior in which they engage and the purpose for which they appear to be designed. Unlike viruses and worms, security risks do not self-replicate.

Symantec AntiVirus can detect, quarantine, delete, and remove or repair the side effects of security risks in the following categories:

- *Spyware*: Stand-alone programs that can secretly monitor system activity and detect information like passwords and other confidential information and relay the information back to another computer.
  Spyware can be unknowingly downloaded from Web sites (typically in shareware or freeware), email messages, and instant messenger software. You may unknowingly download spyware by accepting an End User License Agreement from a software program.
- *Adware*: Stand-alone or appended programs that can secretly gather personal information through the Internet and relay it back to another computer. Adware may track browsing habits for advertising purposes. Adware can also deliver advertising content.
  Adware can be unknowingly downloaded from Web sites (typically in shareware or freeware), email messages, and instant messenger software. You may unknowingly download adware by accepting an End User License Agreement from a software program.
- *Dialers*: Programs that use a computer, without your permission or knowledge, to dial out through the Internet to a 900 number or FTP site, typically to accrue charges.
- *Hack tools*: Programs that are used by a hacker to gain unauthorized access to your computer. For example, one hack tool is a keystroke logger, which tracks and records individual keystrokes and can send this information back to the hacker. The hacker can then perform port scans or vulnerability scans. Hack tools may also be used to create tools for virus creation.
- *Joke programs*: Programs that can alter or interrupt the operation of a computer in a way that is intended to be humorous or frightening. For example, a program can be downloaded from Web sites (typically in shareware or freeware), email messages, or instant messenger software. It can then move the trash can away from the mouse when you attempt to delete or cause the mouse to click in reverse.
- *Other*: Security risks that do not conform to any other security risk category, but that may present a security risk to your computer and its data.

- *Remote access*: Programs that allow access over the Internet from another computer to gain information or to attack or alter your computer. For example, you may install a program, or it may be installed as part of some other process without your knowledge. The program can be used for malicious purposes with or without modification of the original remote access program.
- *Trackware*: Stand-alone or appended applications that trace a user's path on the Internet and send information to a target system. For example, the application can be downloaded from Web sites, email messages, or instant messenger software. It can then obtain confidential information regarding user behavior.

By default, all Symantec AntiVirus scans, including Auto-Protect scans, check for viruses, Trojan horses, worms, and all categories of security risks.

See "Using Auto-Protect" on page 47.

See "Initiating manual scans" on page 56.

The Symantec™ Security Response Web site provides the latest information about threats and security risks. The Web site also contains extensive reference information, such as white papers and detailed information about viruses and security risks.

Figure 1-1 shows information about a hack tool and how Symantec Security Response suggests that you handle it.

Figure 1-1 Symantec Security Response security risk description

See “Accessing the Symantec Security Response Web site” on page 42.

How Symantec AntiVirus responds to viruses and security risks

Symantec AntiVirus safeguards computers from viruses and security risks no matter what the source. Computers are protected from viruses and security risks that spread from hard drives and floppy disks, and others that travel across networks. Computers are also protected from viruses and security risks that spread through email attachments or some other means. For example, a security risk may install itself on your computer without your knowledge when you access the Internet.

Files within compressed files are scanned and cleaned of viruses and security risks. No separate programs or options changes are necessary for Internet-borne viruses. Auto-Protect scans uncompressed program and document files automatically as they are downloaded.

Symantec AntiVirus responds to files that are infected by viruses or by security risks with first actions and second actions.

When a virus is detected during a scan, Symantec AntiVirus, by default, attempts to clean the virus from the infected file and repair the effects of the virus. If the file is cleaned, the virus is successfully and completely removed. If for some reason Symantec AntiVirus cannot clean the file, Symantec AntiVirus attempts the second action, moving the infected file to the Quarantine so that the virus cannot spread.

When your virus protection is updated, Symantec AntiVirus automatically checks to see if any files are stored in the Quarantine and gives you the option of scanning them using the new protection information.

Note: Your administrator may choose to scan files in the Quarantine automatically.

By default, for security risks, Symantec AntiVirus quarantines the infected files and returns the system information that the security risk has changed to its previous state. Some security risks cannot be completely removed without causing another program on your computer, such as a Web browser, to fail. If Symantec AntiVirus is not configured to handle the risk automatically, it prompts you before it stops a process or restarts your computer. Alternatively, you can configure Symantec AntiVirus to use the log only action for security risks.

When Symantec AntiVirus discovers security risks, it also presents a link in the scan window to Symantec Security Response, where you can learn more about the security risk. Your system administrator may also send a customized message.

How Symantec AntiVirus protects your computer

Virus infections can be avoided. Viruses that are quickly detected and removed from your computer cannot spread to other files and cause damage. The effects of viruses and security risks can be repaired. When a virus or a security risk is detected, by default Symantec AntiVirus notifies you that one or more of your files is affected. If you do not want to be notified, you or your administrator can configure Symantec AntiVirus to handle the risk automatically.

Symantec AntiVirus provides these types of protection:

- Auto-Protect: Constantly monitors activity on your computer by looking for viruses and security risks when a file is executed or opened, and when modifications have been made to a file, such as renaming, saving, moving, or copying a file to and from folders.
- Signature-based scanning: Searches for residual virus signatures in infected files, and for the signatures of security risks in infected files and system information. This search is called a *scan*. Depending on how your computer is managed, you and your company's administrator can initiate signature-based or pattern-based scans to systematically check the files on your computer for viruses and security risks, such as adware or spyware. Scans can be run on demand, scheduled to run unattended, or run automatically at system startup.
- Advanced heuristics: Analyzes a program's structure, its behavior, and other attributes for virus-like characteristics. In many cases it can protect against threats such as mass-mailing worms and macro viruses, if you encounter them before updating your virus definitions. Advanced heuristics looks for script-based threats in HTML, VBScript, and JavaScript files.

What keeps Symantec AntiVirus protection current

Symantec engineers track reported outbreaks of computer viruses to identify new viruses. They also track new security risks, such as adware and spyware. After a virus or security risk is identified, a *signature* (information about the virus or security risk) is stored in a *definitions file*, which contains the necessary information to detect, eliminate, and repair the effects of the virus or security risk. When Symantec AntiVirus scans for viruses and security risks, it is searching for these types of signatures.

Symantec makes updated definitions available on an ongoing basis. Definitions are updated daily on the Symantec Security Response Web site. New definitions are made available at least weekly for delivery using LiveUpdate, and whenever a destructive new virus appears.

When new viruses and security risks are so complex that issuing new definitions files for them isn't sufficient, Symantec engineers can update the AntiVirus Engine with the latest detection and repair components. When necessary, AntiVirus Engine updates are included with the definitions files.

About the role of Symantec Security Response

The strength behind Symantec AntiVirus is Symantec Security Response. The increasing number of computer viruses and security risks requires great effort to track, identify, and analyze, and to develop new technologies to protect your computer.

Symantec Security Response researchers disassemble each virus and security risk sample to discover its identifying features and behavior. With this information, they develop definitions that Symantec products use to detect, eliminate, and repair the effects of new viruses and security risks during scans.

Because of the speed at which new viruses spread, particularly over the Internet, Symantec Security Response has developed automated software analysis tools. With direct submissions over the Internet of infected files from your Central Quarantine to Symantec Security Response, the time from discovery to analysis to cure is shrinking from days to hours, and in the near future, to minutes.

Symantec Security Response researchers also research and produce technologies to protect computers from security risks such as spyware, adware, and hack tools.

Symantec Security Response maintains an encyclopedia that provides detailed information about viruses and security risks. In necessary cases, they provide information about removing or uninstalling the risk. The encyclopedia is located on the Symantec Security Response Web site.

See "Accessing the Symantec Security Response Web site" on page 42.

How virus and security risk protection is updated

Your administrator determines how your virus and security risk definitions are updated. You may not have to do anything to receive new definitions.

The LiveUpdate feature in Symantec AntiVirus can be set up by your administrator to make sure that your virus and security risk protection remains current. With LiveUpdate, Symantec AntiVirus connects automatically to a special Web site, determines if your files need updating, downloads the proper files, and installs them in the proper location.

See "Keeping virus and security risk protection current" on page 37.

Chapter 2

Symantec AntiVirus basics

This chapter includes the following topics:

About content licensing

A content license is a grant by Symantec Corporation to update computers using Symantec software. Content licensing ensures that Symantec products receive the latest updates for a specified period of time. Content updates include virus and security risk definitions.

A content license must be allocated to or installed on each computer that is running Symantec AntiVirus.

Note: In some enterprises, Symantec content updates are governed by a site license. In these cases, content licenses are not applied and you do not need to refer to this section.

Symantec clients can receive one content update without a content license. This ensures that newly installed software can provide the most current protection while giving you time to request a content license from Symantec for future updates. Thereafter, computers without valid content licenses do not receive content updates.

Content licenses are installed in the following ways:

- For clients managed through Symantec System Center, a client receives its license seat automatically when it checks in with its parent server. You do not have to do anything to install a content license.
- For clients managed with third-party distribution tools, your administrator will ensure that your client receives a license automatically. You do not have to do anything to install a content license.
- For unmanaged clients, where Symantec System Center is not used, you install the content license file. Your administrator will either provide a content license file or notify you of the location of the content license file for installation.

Installing a content license to an unmanaged client

Your administrator will provide a content license file in one of the following ways:

- Send you the content license file by email.
- Place the content license file on a network drive and notify you of the location.

To install a content license to an unmanaged client

1. In Symantec AntiVirus, click **View** > **License**.
2. In the right pane, click **Install License**.
3. In Step 1 of the License Install Wizard, click **Browse** to locate the content license file, and then click **Next**.
4. In Step 2 of the License Install Wizard, confirm the license information, and then click **Next**.
5. To close the License Install Wizard, click **Finish**.

Opening Symantec AntiVirus

You can open Symantec AntiVirus in several ways.

To open Symantec AntiVirus

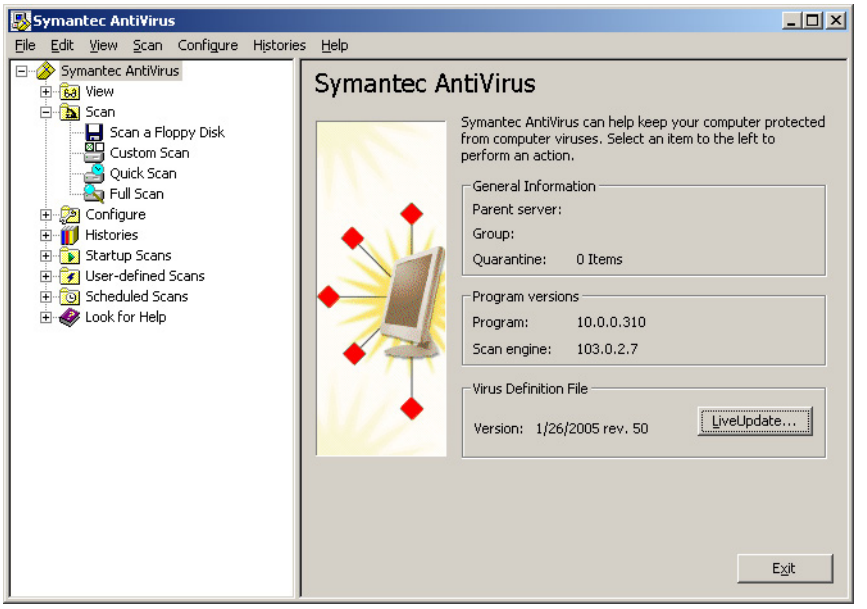
- Do one of the following:
  - On the Windows® taskbar, double-click the Symantec AntiVirus icon.

    Your administrator determines whether this icon appears on the taskbar.
  - On the Windows or Windows XP taskbar, click **Start** > **Programs** > **Symantec Client Security** > **Symantec AntiVirus** or **Start** > **More Programs** > **Symantec Client Security** > **Symantec AntiVirus**, as appropriate.

Navigating in the Symantec AntiVirus main window

The Symantec AntiVirus main window is divided into two panes. The left pane groups activities that you can perform into categories. For example, Scan a Floppy Disk, Custom Scan, Quick Scan, and Full Scan are tasks in the Scan category. Individual icons represent each category in the left pane. When you select categories and other items in the left pane, the right pane displays the information that you need to perform a task.



To navigate in the Symantec AntiVirus main window

- In the left pane, do any of the following:
  - Click a plus sign to expand a folder.
  - Click a minus sign to collapse a folder.
  - Select an item to access the information in the right pane.

Viewing Symantec AntiVirus categories

The activities that you can perform using Symantec AntiVirus are organized into several main categories. Each category has a number of options that you can set.

The following tables do not discuss the individual options that you can change, but give a general description of what they do and how you can find them. For specific information about an option, see the online Help.

View category

You can use the View category to keep track of antivirus and security risk activities.

Table 2-1 View category

Option	Description
Auto-Protect Scan Statistics	View statistics about the status of Auto-Protect scans, including the last file that was scanned (even if it wasn't infected).
Scheduled Scans	View the list of all scheduled scans created to run on your computer, including the name of the scan, when it is scheduled to run, and who created it. A scheduled scan may be created by you or your company's administrator.
Quarantine	Manage infected files that have been isolated to prevent the spread of viruses or the effects of security risks. See "Rescanning files in the Quarantine for viruses" on page 83.

Table 2-1 View category

Option	Description
Backup Items	Delete backup copies of infected files. As a data safety precaution, Symantec AntiVirus makes a backup copy of infected items before attempting a repair. After verifying that Symantec AntiVirus cleaned an item infected by a virus, you should delete the copy in Backup Items. Symantec AntiVirus backs up files that are infected by security risks when the files are put into Quarantine. It also keeps copies of the registry settings and system load points that are affected by security risks such as spyware and adware. System load points are areas of software that are particularly vulnerable to security risks. **Note:** In some cases, deleting a security risk can cause applications to lose functionality. Make sure that you do not need the security risk item to run any applications before you delete it to free up disk space. See "Clearing Backup Items" on page 86.
Repaired Items	Items that have been cleaned or repaired, and whose original locations are no longer available, such as a network drive. For example, an infected attachment may have been stripped from an email message and quarantined. After the item is cleaned in the Quarantine and moved to Repaired Items, you must restore the item from Repaired Items and specify the location to which to restore it.
License Applies only to content licenses; item does not appear in menu if using a site license.	View information about the current license. Current license information includes the license status, serial number, and start and expiration dates. You can start the license installation wizard.

Scan category

You can use the Scan category to perform a manual scan of your computer.

Table 2-2 Scan category

Option	Description
Scan a Floppy Disk	Scan floppy disks and other removable media.

Table 2-2 Scan category

Option	Description
Custom Scan	Perform a manual scan of a file, folder, drive, or entire computer at any time. See "Initiating manual scans" on page 56.
Quick Scan	Perform a very rapid scan of system memory and all of the common virus and security risk locations on the computer.
Full Scan	Perform a full scan of your system, including the boot sector and system memory. A password might be required to scan network drives.

Configure category

You can use the Configure category to set up Auto-Protect to monitor your files and email attachments (for supported email clients) and to set up Tamper Protection to protect Symantec applications from tampering.

Table 2-3 Configure category

Option	Description
File System Auto-Protect	Whenever you access, copy, save, move, or open a file, it is examined to ensure that it is not infected by a virus or security risk. Auto-Protect includes the SmartScan feature which, when enabled, can determine a file's type even when a virus changes the file's extension. See "Using Auto-Protect" on page 47.
Internet E-mail Auto-Protect Lotus Notes® Auto-Protect Microsoft® Exchange Auto-Protect	For groupware email clients (Lotus Notes and Microsoft Exchange/Microsoft Outlook® clients), Symantec AntiVirus includes additional protection for email. For Internet E-mail clients, Symantec AntiVirus protects incoming and outgoing email messages that use the POP3 or SMTP communications protocol.
Tamper Protection	Tamper Protection protects Symantec applications from tampering by unauthorized sources.

Histories category

You can use the Histories category to track information about the scans that run on your computer, and virus infections and security risks that are found.

Table 2-4 Histories category

Option	Description
Risk History	View a list of the following items: ■ The viruses that have infected your computer, with additional relevant information about the infection. ■ The security risks, such as adware and spyware, that Symantec AntiVirus detected and logged, or quarantined and repaired, or deleted on your computer. The Risk History for security risks includes a link to the Symantec Security Response Web page that provides additional information.
Scan Histories	Keep track of the scans that have occurred on your computer over time. Scans are displayed with additional relevant information about the scans.
Event Log	View a log of activities on your computer that are related to viruses and security risks, including configuration changes, errors, and definitions file information.
Tamper History	View a list of the attempts to tamper with the Symantec applications on your computer that have been thwarted by Tamper Protection.

Startup Scans category

You can use the Startup Scans category to create and configure scans to run when you start your computer.

Table 2-5 Startup Scans category

Option	Description
New Startup Scan	Some users supplement a scheduled scan with an automatic scan whenever they start their computers. Often, a startup scan is restricted to critical, high-risk folders, such as the Windows folder and folders that store Microsoft Word and Excel templates. See "Creating startup scans" on page 61.

Table 2-5 Startup Scans category

Option	Description
Auto-Generated QuickScan	This scan checks the files in memory and other common infection points on the computer for viruses and security risks each time that a user logs on to the computer. You can configure this scan in the same way that you can configure any manual scan, except that you cannot stop it from scanning the files in memory and other common infection points on the computer. **Note:** This type of scan is available only on unmanaged clients.

User-defined Scans category

You can use the User-defined Scans category to create preconfigured scans that you can run manually.

Table 2-6 User-defined Scans category

Option	Description
New User-defined Scan	If you regularly scan the same set of files or folders, you can create a scan that is restricted to those items. At any time, you can quickly verify that the specified files and folders are free of viruses and security risks. See "Creating user-defined scans" on page 62.

Scheduled Scans category

You can use the Scheduled Scans category to create preconfigured scans that run automatically at the times that you specify.

Table 2-7 Scheduled Scans category

Option	Description
New Scheduled Scan	Schedule a scan of your hard disks that runs at least once a week. A scheduled scan confirms that your computer remains free of viruses and security risks. See "Creating scheduled scans" on page 59.

Enabling and disabling Auto-Protect

If you have not changed the default option settings, Auto-Protect loads when you start your computer to guard against viruses and security risks. It checks programs for viruses and security risks as they run and monitors your computer for any activity that might indicate the presence of a virus or security risk. When a virus, *virus-like activity* (an event that could be the work of a virus), or security risk is detected, Auto-Protect alerts you.

In some cases, Auto-Protect may warn you about a virus-like activity that you know is not the work of a virus. For example, this might occur when you are installing new computer programs. If you will be performing such an activity and want to avoid the warning, you can temporarily disable Auto-Protect. Be sure to enable Auto-Protect when you have completed your task to ensure that your computer remains protected.

Your administrator might lock Auto-Protect so that you cannot disable it for any reason, or specify that File Auto-Protect can be disabled temporarily, but reenables automatically after a specified amount of time.

Enable and disable File System Auto-Protect

The Symantec AntiVirus icon is displayed on the taskbar in the lower-right corner of your Windows desktop. In some configurations, the icon is not displayed.

The Symantec AntiVirus icon appears as a full shield. When you right-click the icon, a check mark appears next to Enable Auto-Protect when File System Auto-Protect is enabled.

The Symantec AntiVirus icon is covered by a universal no sign, a red circle with a diagonal slash, when File System Auto-Protect is disabled.

To enable and disable File System Auto-Protect from the taskbar

- On the Windows desktop, in the system tray, right-click the Symantec AntiVirus icon, and then click **Enable Auto-Protect**.

To enable and disable File System Auto-Protect from Symantec AntiVirus

1. In Symantec AntiVirus, in the left pane, click **Configure**.
2. In the right pane, click **File System Auto-Protect**.
3. Check or uncheck **Enable Auto-Protect**.
4. Click **OK**.
   The current File System Auto-Protect status updates dynamically to the right of the check box.

Pausing and delaying scans

The Pause feature lets you stop a scan at any point during the scan and resume it at another time. You can pause any scan that you initiate. Your network administrator determines whether you can pause an administrator-scheduled scan.

For scheduled scans that your network administrator initiates, you may also be allowed to delay the scan. If your administrator has enabled the Snooze feature, you can delay an administrator-scheduled scan for a set interval of time. When the scan resumes, it restarts from the beginning.

Pause the scan if you're planning on resuming it after a temporary break. Use the Snooze feature to delay the scan for a longer period of time during which you don't want to be interrupted, for example, if you're in the middle of a presentation.

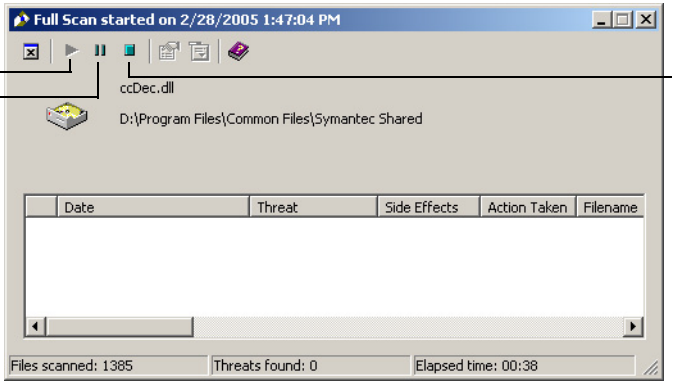
Pause or delay a scan

Use the following procedures to pause a scan initiated by you or delay an administrator-scheduled scan. If the Pause the Scan button is not available, your network administrator has disabled the Pause feature.

Note: If Symantec AntiVirus is scanning a compressed file when you choose to pause a scan, it may take several minutes to respond.

To pause a scan

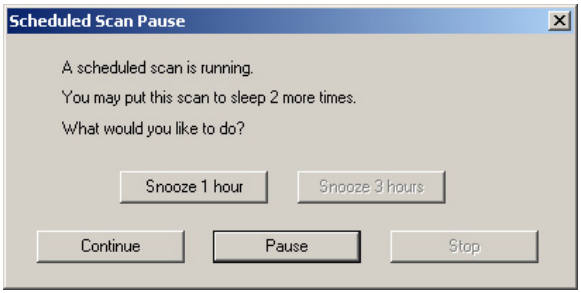
1 When the scan runs, in the scan dialog box, click the pause icon.



The buttons that display in a scan dialog box are the same whether it's a scan that you initiate or an administrator-initiated scan

If it's a scan that you initiated, the scan stops where it is and the scan dialog box remains open until you start the scan again.

If it's an administrator-scheduled scan, the Scheduled Scan Pause dialog box appears.



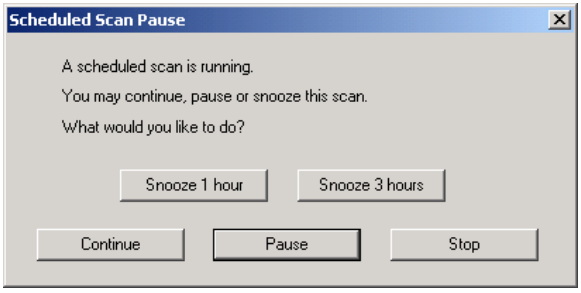
2 In the Scheduled Scan Pause dialog box, click **Pause**.
The administrator-scheduled scan stops where it is and the scan dialog box remains open until you start the scan again.

3 In the scan dialog box, click the start icon to continue the scan.

To delay an administrator-scheduled scan

1 When the administrator-scheduled scan runs, in the scan dialog box, click **Pause the Scan**.

2 In the Scheduled Scan Pause dialog box, click **Snooze 1 hour** or **Snooze 3 hours**.



Your administrator specifies the period of time that you're allowed to delay the scan. When you've reached that set period of time, the scan restarts from the beginning. Your administrator specifies the number of times that you can delay the scheduled scan before this feature is disabled.

Keeping virus and security risk protection current

Symantec AntiVirus relies on up-to-date information to detect, eliminate, and repair the effects of viruses and security risks. One of the most common reasons that virus or security risk problems occur is that definitions files are not updated after installation. The definitions files contain the necessary detection and repair information about all newly discovered viruses and security risks.

Symantec supplies updated definitions files weekly through LiveUpdate and daily through Intelligent Updater files posted to the Symantec Security Response Web site. Updates are also issued whenever a new high-risk virus threat emerges. Make it a practice to update definitions once a week at a minimum. Scheduling LiveUpdate to run automatically is the easiest way not to forget. Always update immediately if a new virus scare is reported.

With LiveUpdate, Symantec AntiVirus connects automatically to a special Symantec Web site, and determines if virus and security risk definitions need to be updated. If so, it downloads the proper files and installs them in the proper location. Generally, you do not have to do anything to configure LiveUpdate. The only requirement is an Internet connection.

Note: Your administrator may have specified a maximum number of days that the virus and security risk definitions can be out of date. After exceeding the maximum number of days, Symantec AntiVirus automatically runs LiveUpdate when an Internet connection is detected.

Scheduling updates with LiveUpdate

By default LiveUpdate is scheduled to run automatically every Friday at 8 p.m. When the scheduled update runs, your computer must be running and have access to the Internet.

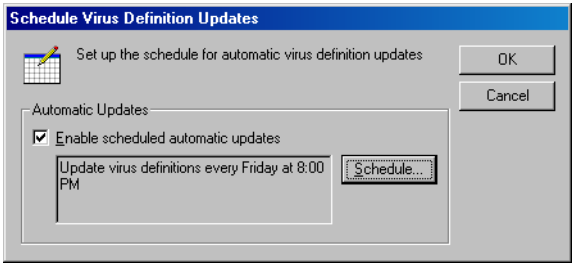
Schedule updates with LiveUpdate

You can change the LiveUpdate frequency and time to fit your needs.

Note: In a centrally managed network, your administrator may distribute updated virus and security risk definitions to workstations. In this case, you do not have to do anything.

To enable scheduled LiveUpdate

1 In Symantec AntiVirus, on the File menu, click **Schedule Updates**.



2 In the Schedule Virus Definition Updates dialog box, check **Enable scheduled automatic updates**.

Note: This updates both virus and security risk definitions.

---

3 Click **OK**.

To set LiveUpdate schedule options

1 In the Schedule Virus Definition Updates dialog box, click **Schedule**.

2 In the Virus Definition Update Schedule dialog box, specify the frequency, day, and time that you want LiveUpdate to run.

3 Click **OK** until you return to the main Symantec AntiVirus window.

To set advanced LiveUpdate schedule options

1 On the File menu, click **Schedule Updates**.

2 In the Schedule Virus Definition Updates dialog box, click **Schedule**.

3 In the Virus Definition Update Schedule dialog box, click **Advanced**.

4 In the Advanced Schedule Options dialog box, do any of the following:

- To set up Symantec AntiVirus so that scheduled LiveUpdate events that are missed run at a later time, check **Handle Missed Events Within** and set the days.
- To set up Symantec AntiVirus so that scheduled LiveUpdate events run within a specified time range rather than at a set time, select the type of randomization method that you want to use and set the minutes, days of the week interval, or number of days of the month to use.

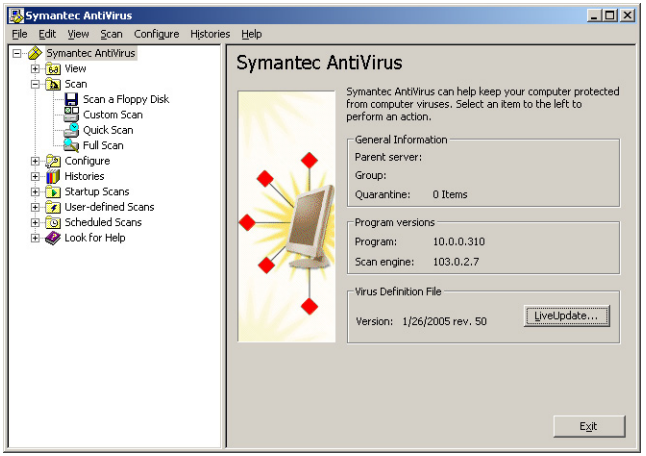
5 Click **OK** until you return to the main Symantec AntiVirus window.

Updating protection immediately with LiveUpdate

When a new virus is reported, do not wait for your next scheduled update. You should update virus and security risk protection immediately.

To update virus protection immediately with LiveUpdate

1 In Symantec AntiVirus, in the left pane, click **Symantec AntiVirus**.



2 In the right pane, click **LiveUpdate**.

3 If necessary, in the LiveUpdate dialog box, click **Options** > **Configure** to customize your Internet connection for LiveUpdate.
You can change your Internet service provider connection or how your computer connects through a proxy server to the Internet.
For more information, use the online Help from LiveUpdate.

4 Click **Next** to start the automatic update.

Updating without LiveUpdate

Symantec supplies a special program called Intelligent Updater as an alternative to LiveUpdate. You can download the updates from the Symantec Security Response Web site.

See "Accessing the Symantec Security Response Web site" on page 42.

To update without LiveUpdate

1. Download the Intelligent Updater program to any folder on your computer.
2. In a My Computer or Windows Explorer window, locate and then double-click the Intelligent Updater program.
3. Follow all prompts displayed by the update program.
   The Intelligent Updater program searches your computer for Symantec AntiVirus, and then installs the new virus and security risk definitions files in the proper folder automatically.
4. Scan your computer to make sure that newly discovered viruses and security risks are detected.

Using Symantec AntiVirus with Windows Security Center

If you are using Windows Security Center (WSC) running on Windows XP Service Pack 2 to monitor security status, you can see Symantec AntiVirus status in WSC.

Table 2-8 shows the protection status reporting in WSC.

Table 2-8 WSC protection status reporting

Symantec product condition	Protection status
Symantec AntiVirus is not installed	NOT FOUND (red)
Symantec AntiVirus is installed with full protection	ON (green)
Symantec AntiVirus is installed, and virus and security risk definitions are out of date	OUT OF DATE (red)
Symantec AntiVirus is installed and File System Auto-Protect is not enabled	OFF (red)
Symantec AntiVirus is installed, File System Auto-Protect is not enabled, and virus and security risk definitions are out of date	OFF (red)
Symantec AntiVirus is installed and Rtvscan is turned off manually	OFF (red)

Table 2-9 shows Symantec™ Client Firewall status reporting in WSC.

Table 2-9 WSC firewall status reporting

Symantec product condition	Firewall status
Symantec Client Firewall is not installed	NOT FOUND (red)
Symantec Client Firewall is installed and enabled	ON (green)
Symantec Client Firewall is installed but not enabled	OFF (red)
Symantec Client Firewall is not installed or enabled, but a third-party firewall is installed and enabled	ON (green)

Note: In Symantec Client Security, Windows Firewall is disabled by default.

If there is more than one firewall enabled, WSC reports that multiple firewalls are installed and enabled.

For more information

If you need more information about Symantec AntiVirus, you can access the online Help. In addition, information about viruses and security risks can be obtained from the Symantec Web site.

Accessing online Help

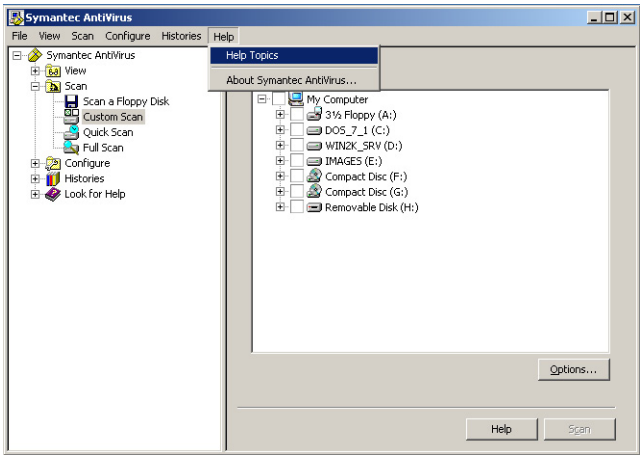
The Symantec AntiVirus online Help system has general information and step-by-step procedures to help you keep your computer safe from viruses and security risks.

Note: Your administrator may have elected not to install the Help files.

To get help using Symantec AntiVirus

- In Symantec AntiVirus, do one of the following:
  - On the Help menu, click **Help Topics**.
  - In the right pane, click **Help**.

Context-sensitive Help is available only in screens on which you can perform actions.



Accessing the Symantec Security Response Web site

If you are connected to the Internet, you can visit the Symantec Security Response Web site to view items such as the following:

- The Virus Encyclopedia, which contains information about all known viruses
- Information about virus hoaxes
- White papers about viruses and virus threats in general
- General and detailed information about security risks

To access the Symantec Security Response Web site

- In your Internet browser, type the following Web address: **securityresponse.symantec.com**

Chapter 3

Protecting your computer from viruses and security risks

This chapter includes the following topics:

About the antivirus and security risk policy

Symantec AntiVirus comes preset with an antivirus and security risk policy that is appropriate for most users. You can change settings based on your personal needs. You can separately customize policy settings for Auto-Protect, manual, scheduled, startup, and user-defined scans.

An antivirus and security risk policy determines:

- What to scan
- What to do if a virus or a security risk is detected

What to scan

Symantec AntiVirus Auto-Protect scans all file types by default. Manual, scheduled, startup, and user-defined scans also examine all file types by default.

Auto-Protect includes SmartScan, which scans files with the extensions included in the Program File Extensions List. SmartScan also scans all executable files and Microsoft® Office documents whether or not the extensions are listed in the Program File Extensions List.

See "Modifying Auto-Protect and using SmartScan" on page 50.

You can choose to scan files by file extension or by type of file (documents and programs), but your protection from viruses and security risks is reduced.

You can also choose to exclude specific files from scanning. For example, if a file that you know is not infected triggers a virus alert during a scan, you prevent further warnings by excluding the file from your subsequent scans.

Scanning by file types or extensions

Symantec AntiVirus can scan your computer by file types or by extensions. Scanning by file types enables Symantec AntiVirus to determine the file's type, regardless of its extension. Because viruses are known to infect only certain types of files, this is a useful scanning method that ensures that all files that are subject to viruses are scanned.

Scanning by file types enables Symantec AntiVirus to scan files that have been renamed by a malicious virus. However, this option is slower than scanning by extensions.

You can choose from the following types of files:

- Document files: Include Microsoft Word and Excel documents, and template files associated with those documents. Symantec AntiVirus searches document files for macro virus infections.
- Program files: Include dynamic-link libraries (.dll), batch files (.bat), communication files (.com), executable files (.exe), and other program files. Symantec AntiVirus searches program files to look for file virus infections.

Scan by file types or extensions

Symantec AntiVirus can scan your computer by file types or by extensions.

To select file types to scan

1. In Symantec AntiVirus, in the left pane, select the scan that you want to change.
   - If you selected a scan from the Scan category, click **Options**.
   - If you selected a startup, user-defined, or scheduled scan, click the specific scan you want, click **Edit**, and then click **Options**.
     Changes will apply only to the specific scan that you select.
2. Click **Selected file types**, and then click **Types**.
3. Select one or both of the following file types:
   - Document files: Include Word and Excel documents, and template files associated with those documents.
   - Program files: Include dynamic-link libraries (.dll), batch files (.bat), communication files (.com), executable files (.exe), and other program files.
4. If you want to use these actions for all subsequent scans, click **Save Settings**.
5. Click **OK**.

To add file extensions to the scan list

1. In Symantec AntiVirus, in the left pane, select the scan that you want to change.
   - If you selected a from the Scan category, click **Options**.
   - If you selected a startup, user-defined, or scheduled scan, click the name of the scan to change, click **Edit**, and then click **Options**.
     Changes apply only to the specific scan that you select.
   - If you selected Auto-Protect, go to step 2.
2. Click **Selected file extensions**, and then click **Extensions**.
3. Type the extension to add, and then click **Add.**
4. Repeat step 3 as needed.
5. Click **OK**.

About scanning all file types

Symantec AntiVirus can scan all of the files on your computer, regardless of extension or file type. Scanning all file types ensures the most thorough scan, because this option enables Symantec AntiVirus to detect viruses and security risks in files that might not otherwise be searched. Scanning by all file types is more time consuming than scanning by selected file types or scanning by file extensions, but it's also more thorough.

If a short scan is important to you, you should set up Auto-Protect scans or idle scans (when available) to scan by extension, and then configure a scheduled scan at least once a week to thoroughly check your computer.

About preventing macro virus infections

The Symantec AntiVirus scanner automatically detects and removes most Microsoft Word and Excel macro viruses. By regularly running scheduled scans, startup scans, or Auto-Protect, you can protect your computer from macro virus infections. Symantec AntiVirus regularly searches and cleans any macro viruses that it detects.

To best prevent macro virus infections, do the following:

- Enable Auto-Protect. Auto-Protect constantly scans files that have been accessed (for example, file execute or file open) or modified (for example, file rename, file modify, file create, file copy, or file moves to a location).
- Run Auto-Protect for your email, if available.
- Set all scan options to scan by All types.
- Protect your global template files by disabling automacros.

What to do if a virus or security risk is detected

Symantec AntiVirus responds to files that are infected by viruses or security risks with a first action and a second action. By default, when a virus is detected by Auto-Protect or during a scan, Symantec AntiVirus attempts to clean the virus from the infected file. If Symantec AntiVirus cannot clean the file, the second action is to log the failed cleaning attempt and move the infected file to the Quarantine so that the virus cannot spread, which denies you further access to the file.

Depending on your antivirus policy, you can change these settings to delete an infected file on detection or leave it alone (log only). For Auto-Protect, you can also choose to deny access. In addition, you can set different actions for macro and nonmacro viruses for each scan type separately.

By default, when a security risk is detected by Auto-Protect or during a scan, Symantec AntiVirus quarantines the infected files and attempts to remove or repair the changes that the security risk has made on the computer. Quarantining the security risk ensures that the security risk is no longer active on your computer, and also ensures that Symantec AntiVirus can reverse the changes, if necessary. If Symantec AntiVirus cannot do this, the second action is to log the risk and leave it alone.

For each scan type, you can change these settings, and set different actions for each category of security risk and for individual security risks as well.

Note: In some instances, you might unknowingly install an application that includes a security risk such as adware or spyware. To avoid leaving the computer in an unstable state, Symantec AntiVirus waits until the application installation is complete before it quarantines the risk. It then removes or repairs the risk's effects.

Using Auto-Protect

Auto-Protect is your best defense against virus attack. Whenever you access, copy, save, move, or open a file, Auto-Protect scans the file to ensure that a virus has not attached itself.

Auto-Protect includes SmartScan, which scans a group of file extensions that contain executable code and all .exe and .doc files. SmartScan can determine a file's type even when a virus changes the file's extension. For example, it scans .doc files even when a virus changes the file extension to one that is different from the file extensions that SmartScan has been configured to scan.

About Auto-Protect and security risks

By default, Auto-Protect scans for security risks such as adware and spyware, quarantines the infected files, and removes or repairs the side effects of the security risks. You can disable scanning for security risks in Auto-Protect.

See "Disabling and enabling security risk scanning in Auto-Protect" on page 50.

About Auto-Protect and email scanning

To supplement Auto-Protect, Symantec Client Security detects at installation whether you use a supported groupware email client and adds Auto-Protect for email. Protection is provided for the following email clients:

- Lotus Notes 4.5x, 4.6, 5.0, and 6.x
- Microsoft Outlook 98/2000/2002/2003 (MAPI and Internet)
- Microsoft Exchange client 5.0 and 5.5

Note: E-mail Auto-Protect works on your supported email client only. It does not protect email servers.

Symantec AntiVirus also includes Auto-Protect scanning for additional Internet email programs by monitoring all traffic that uses the POP3 or SMTP communications protocols. You can configure Symantec AntiVirus to scan incoming messages for threats and security risks, as well as outgoing messages for known heuristics by using Bloodhound™ Virus Detection. Scanning outgoing email helps to prevent the spread of threats such as worms that can use email clients to replicate and distribute themselves across a network.

Note: Internet email scanning is not supported for 64-bit computers.

For Lotus Notes and Microsoft Exchange email scanning, Symantec AntiVirus scans only the attachments that are associated with email. For Internet email scanning of messages that use the POP3 or SMTP protocols, Symantec AntiVirus scans both the body of the message and any attachments that are included.

When Auto-Protect is enabled for a supported email client and you open a message with an attachment, the attachment is immediately downloaded to your computer and scanned. Over a slow connection, downloading messages with large attachments affects mail performance. You may want to disable this feature if you regularly receive large attachments.

There are times, such as during the installation of new software, that you must temporarily disable Auto-Protect.

See "Enabling and disabling Auto-Protect" on page 34.

Note: If a virus is detected as you open email, your email may take several seconds to open while Symantec AntiVirus completes its scan.

Email scanning does not support the following email clients:

- IMAP clients
- AOL® clients
- POP3 that uses Secure Sockets Layer (SSL)
- Web-based email such as Hotmail® and Yahoo!® Mail

Disabling email scanning if you use SSL connections

If your Internet service provider uses the SSL protocol, you might have problems sending email messages when Symantec AntiVirus email scanning is enabled. In this case, you might need to disable Symantec AntiVirus email scanning.

File System Auto-Protect continues to protect your computer from viruses and security risks in attachments even after you disable Internet E-mail client scanning. File System Auto-Protect scans email attachments when you save the attachments to the hard drive.

After you disable the email scanner, be sure that Auto-Protect is enabled, and run LiveUpdate regularly to ensure that Auto-Protect has been optimally configured. Auto-Protect provides real-time virus protection from any source, including the Internet, and automatically scans email attachments whenever they are accessed.

To disable email scanning

1. In Symantec AntiVirus, in the left pane, click **Configure**.
2. In the right pane, click **<Email> Auto-Protect**.
3. Uncheck **Enable <Email> Auto-Protect**.
4. Click **OK**.

Viewing Auto-Protect Scan Statistics

Auto-Protect Scan Statistics displays the status of the last Auto-Protect scan, the last file that was scanned, and virus infection and security risk information.

To view Auto-Protect Scan Statistics

- In Symantec AntiVirus, on the View menu, click **Auto-Protect Scan Statistics**.

Modifying Auto-Protect and using SmartScan

Auto-Protect is preset to scan all files. Scanning all files and using SmartScan offers the most protection from viruses and security risks. SmartScan is enabled by default.

Symantec AntiVirus may complete scans faster by scanning only files with selected extensions, such as .exe, .com, .dll, .doc, and .xls. Although this method offers less protection, it is an efficient way to scan for viruses because viruses affect only certain file types. The default list of extensions represents those files that are commonly at risk of infection by viruses.

To modify Auto-Protect and use SmartScan

1. In Symantec AntiVirus, in the left pane, click **Configure**.
2. In the right pane, click **File System Auto-Protect**.
3. In the File Types group box, do one of the following:
   - Click **All Types** to scan all files.
   - Click **Selected** to scan only those files that match the listed file extensions, and then click **Extensions** to change the default list of file extensions.
   - Ensure that SmartScan is checked to scan using this feature.
4. Click **OK** to save your settings.

Disabling and enabling security risk scanning in Auto-Protect

By default, Auto-Protect scans for security risks such as adware and spyware, quarantines infected files, and attempts to remove or repair the effects of the security risk. From time to time, however, you might need to temporarily disable scanning for security risks in File System Auto-Protect, and then reenable it.

Note: Your administrator might lock this setting.

To disable and enable security risk scanning in Auto-Protect

1. In Symantec AntiVirus, in the left pane, click **Configure**.
2. In the right pane, click **File System Auto-Protect**.
3. Under Options, check or uncheck **Scan for Security Risks**.
4. Click **OK**.

Using Tamper Protection

Tamper Protection protects Symantec applications from tampering by worms, Trojan horses, viruses, and security risks.

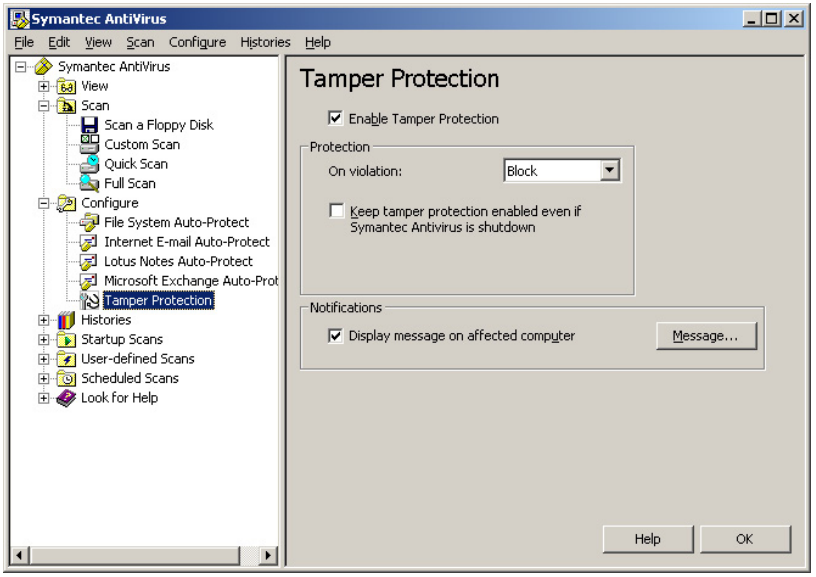
Enabling, disabling, and configuring Tamper Protection

When Tamper Protection is enabled, you can configure Symantec AntiVirus to block or log attempts to modify Symantec applications. You can also configure a message to appear on your computer when Symantec AntiVirus detects a tampering attempt.

Note: If an administrator manages your computer, and the Tamper Protection options display a padlock icon, you cannot change these options because your administrator has locked them.

To enable, disable, and configure Tamper Protection

1 In Symantec AntiVirus, in the left pane, click **Tamper Protection**.



2 In the right pane, check or uncheck **Enable Tamper Protection**.

3 If you enabled Tamper Protection, then under Protection, in the drop-down list, do one of the following:

- To block unauthorized activity, click **Block**.
- To log unauthorized activity but allow the activity to take place, click **Log Only**.

4 Check or uncheck **Keep Tamper Protection enabled even if Symantec AntiVirus is shut down**.

5 Under Notifications, check or uncheck **Display message on affected computer**.

6 Click **OK**.

Creating Tamper Protection messages

Tamper Protection lets you create a message that appears when Tamper Protection detects attacks against Symantec processes. The message that you create can contain a mix of text that you type and fields that you select. The fields that you select are variables that are populated by values that identify characteristics of the attack.

Table 3-1 describes the fields that you can select.

Table 3-1 Tamper Protection message field names and descriptions

Field	Description
Filename	The name of the file that attacked protected processes.
PathAndFilename	The complete path and name of the file that attacked protected processes.
Location	The area of the computer hardware or software that was protected from tampering. For Tamper Protection messages, this is Symantec applications.
Computer	The name of the computer that was attacked.
User	The name of the logged on user when the attack occurred.
DateFound	The date on which the attack occurred.
Action Taken	The action that Tamper Protection performed to respond to the attack.
System Event	The type of tampering that occurred.
Entity Type	The type of target that the process attacked.
Actor Process ID	The ID number of the process that attacked a Symantec application.

Table 3-1 Tamper Protection message field names and descriptions

Field	Description
Actor Process Name	The name of the process that attacked a Symantec application.
Target Pathname	The location of the target that the process attacked.
Target Process ID	The process ID of the target that the process attacked.
Target Terminal Session ID	The ID of the terminal session on which the event occurred.

Use the following format to create messages:

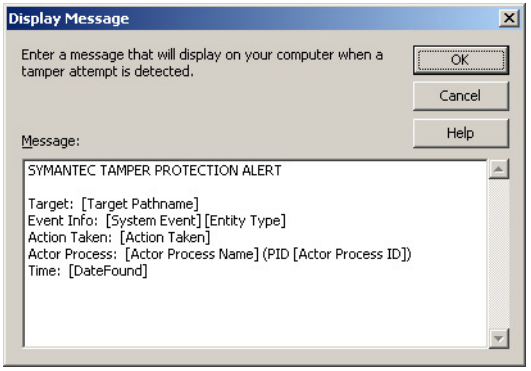
```
Text that you type: [Field Name 1] [Field Name 2] (Optional and
additional text that you type [Field Name x])
```

The following example illustrates a message that tells you which process attempted to take which action and when:

```
Date: [DateFound]
Process Located At: [PathAndFilename] (Named: [Actor Process Name])
Attacked: [Target Pathname] [Target Process ID]
```

To create Tamper Protection messages

1. In Symantec AntiVirus, in the left pane, click **Tamper Protection**.
2. In the right pane, under Notifications, ensure that **Display message on affected computer** is checked, and then click **Message**.



3. In the Message box, click to insert a cursor.
4. Use your keyboard to move the cursor, add rows, and type and delete text.

5 Move the cursor to a position in which you want to insert a field, right-click, click **Insert Field**, and then select the field to insert.
See "Tamper Protection message field names and descriptions" on page 52.

6 Repeat steps 4 and 5 as necessary.

7 In the field, right-click, and then select Cut, Copy, Paste, Clear, or Undo.

8 Click **OK**.

Scanning for viruses and security risks

In addition to Auto-Protect, which is your most powerful defense against virus infection and security risks, Symantec AntiVirus supplies several different types of scans to provide additional protection. Available scans include the following:

- Custom Scan: Scan a file, folder, drive, or entire computer at any time. You select the parts of the computer to scan.
- Quick Scan: Quickly scan system memory and locations that viruses and security risks commonly attack.
- Full Scan: Scan the entire computer, including the boot sector and system memory. You might need to enter a password to scan network drives.
- Scheduled scans: Run unattended at a specified frequency.
- Startup scans: Run every time you start your computer and Windows loads.
- User-defined scans: Scan specified file sets at any time.

A daily Quick Scan and a single, weekly scheduled scan of all files is generally sufficient protection, as long as Auto-Protect is always running. If your computer is frequently attacked by viruses, consider adding a full scan at startup or daily scheduled scan. Another good habit is to always scan floppy disks when first used, particularly if they have been circulating among users.

How Symantec AntiVirus detects viruses and security risks

Symantec AntiVirus prevents virus infections on a computer by scanning the computer's boot sector, memory, and files for viruses and security risks. The Symantec AntiVirus Scan Engine uses virus and security risk signatures that are found in definitions files to do an exhaustive search for known viruses that are inside executable files. Symantec AntiVirus searches the executable parts of document files to find macro viruses.

You can perform a scan while you wait or schedule a scan for when you are away from your desk.

What happens during a scan

During a scan, Symantec AntiVirus searches the computer's memory, boot sector, and selected drives for virus and security risk signatures that identify an infection or the presence of a risk.

Computer memory

Symantec AntiVirus searches the computer's memory. Any file virus, boot sector virus, or macro virus may be memory-resident. Viruses that are memory-resident have copied themselves into a computer's memory. In memory, a virus can hide until a trigger event occurs. Then the virus can spread to a floppy disk in the disk drive, or to the hard drive. There is no known way to clean viruses that find their way to memory. However, you can remove a virus from memory by restarting your computer when prompted.

Boot sector

Symantec AntiVirus checks the computer's boot sector for boot viruses. Two items are checked: the partition tables and the master boot record.

Floppy drive

A common way for a virus to spread is through floppy disks that are left in a disk drive when a computer is being turned on or off. If a floppy disk is in the disk drive when a scan is started, Symantec AntiVirus searches the boot sector and partition tables of the floppy drive. If a floppy disk is in the disk drive when you turn off your computer, you are prompted to remove the disk to prevent possible infection.

Selected files

Symantec AntiVirus scans individual files. For most types of scans, you select the files that you want scanned. Symantec AntiVirus uses pattern-based scanning to search for traces of viruses, called patterns or signatures, within files. Each file is compared to the innocuous signatures that are contained in a virus definitions file, as a way of identifying specific viruses. If a virus is found, by default Symantec AntiVirus attempts to clean the virus from the file. If the file cannot be cleaned, Symantec AntiVirus quarantines the file to prevent further infection of your computer.

Symantec AntiVirus also uses pattern-based scanning to search for signs of security risks within files and registry keys. If a security risk is found, by default Symantec AntiVirus quarantines the infected files and repairs the risk's effects. If this cannot be done, it logs the attempt.

At the end of the scan, results are listed.

About definitions files

Virus files include bits of code that, when broken down, display certain patterns (also called signatures). These virus patterns can be traced in infected files. Security risks, such as adware and spyware, also have recognizable patterns or signatures.

The definitions file contains a list of known virus patterns or signatures, without the harmful virus code, and known signatures for security risks. The scanner searches for known patterns that are found in the definitions file within files on your computer. If a virus match is found, the file is infected. Symantec AntiVirus uses the definitions file to determine which virus caused the infection and to repair its side effects. If a security risk is found, Symantec AntiVirus uses the definitions file to quarantine it and repair its side effects.

Because new viruses and security risks are introduced into the computer community almost every day, definitions files must be updated regularly to ensure that Symantec AntiVirus can detect and clean even the most recent viruses and security risks.

About scanning compressed and encoded files

Symantec AntiVirus scans within compressed and encoded files, for example, .zip files. Your administrator can specify scanning up to 10 levels deep for compressed files that contain compressed files. Check with your administrator for the types of compressed file scans that are supported.

If Auto-Protect is enabled, any file that is removed from a compressed file is scanned, thereby protecting your computer.

Initiating manual scans

You can manually scan for viruses and security risks, such as adware and spyware, at any time. Select anything to scan from a single file to a floppy disk to your entire computer. Manual scans include the Quick Scan and Full Scan.

Initiate manual scans

You can initiate scans from the My Computer window, the Windows Explorer window, or the Symantec AntiVirus main window.

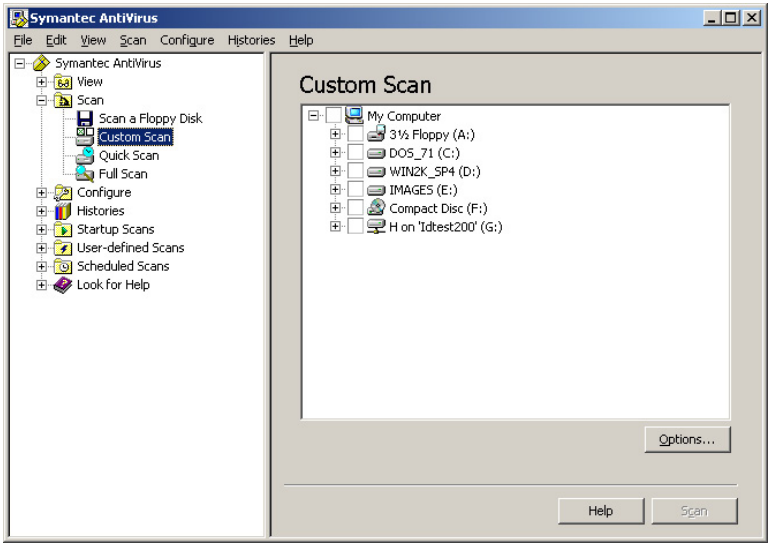
To initiate a manual scan from Windows

- In a My Computer window or Windows Explorer window, right-click a file, folder, or drive, and then click **Scan For Viruses**.

Note: This feature is not supported on 64-bit operating systems.

To initiate a manual scan within Symantec AntiVirus

1. In Symantec AntiVirus, in the left pane, expand **Scan**.
2. In the left pane, select one of the following:
   - Scan a Floppy Disk
     This option is available only when a floppy disk drive is present.
   - Custom Scan
   - Quick Scan
   - Full Scan



3 If you selected Scan a Floppy Disk or Custom Scan, in the right pane, do the following:

- Double-click a drive or folder to open or close it.
- Check or uncheck items that you want to scan.
  The symbols mean the following:


The file, drive, or folder is not selected. If the item is a drive or folder, the folders and files in it are also not selected.


The individual file or folder is selected.


The individual folder or drive is selected. All items within the folder or drive are also selected.


The individual folder or drive is not selected, but one or more items within the folder or drive are selected.

4 For all manual scans, click **Options** to change the default settings for what is scanned and how to respond if a virus or security risk is detected.
The default settings are as follows:

- The default setting is to scan all files.
- For viruses, the default settings for actions are to clean the virus from an infected file and repair its effects, and quarantine the infected file if the virus cannot be removed.
- For security risks, the default settings for actions are to quarantine the security risk and repair its side effects, or log the risk if it cannot be quarantined and repaired.

To apply the modified settings only to the current scan, click **OK**. To apply the settings to all future scans, click **Save Settings**.

5 Click **Advanced** to configure a scan progress dialog box to appear during the scheduled scan.

6 In the Scan Advanced Options dialog box, under Dialog options, in the drop-down list, click **Show scan progress**, and then click **OK**.

7 In the Scan Options dialog box, click **OK**.

8 In the Symantec AntiVirus main window, click **Scan**.
Symantec AntiVirus begins the scan and reports the results.

Configuring scanning

You can configure several different kinds of scans to protect your computer against viruses and security risks.

Creating scheduled scans

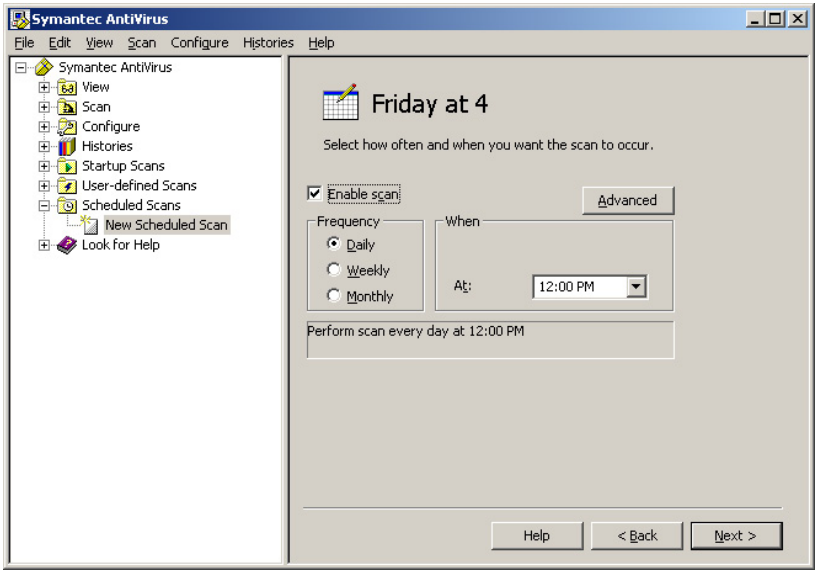
A scheduled scan is an important component of threat and security risk protection. At the very least, schedule a scan to run once a week to ensure that your computer remains free of viruses and security risks, such as adware and spyware.

Note: If your network administrator has created a scheduled scan for you, it appears in the Scheduled Scans area of the View folder, not in the Scheduled Scans folder. The Scheduled Scans folder only displays scans that you've scheduled.

To create a scheduled scan

1. In Symantec AntiVirus, in the left pane, click **Scheduled Scans**.
2. In the right pane, click **New Scheduled Scan**.
3. Select one of the following types of scan to schedule:
   - Quick Scan
   - Full Scan
   - Custom Scan
4. Click **Next**.
5. Type a name and description for the scan.
   For example, call the scan "Friday at 4."
6. Click **Next**.

7 Specify the frequency and when to scan, and then click **Next**.



8 If you selected Custom Scan, then in the right pane, check the appropriate check boxes to specify where to scan.
You can check anything from the entire computer to a single file.
See "Initiating manual scans" on page 56.

9 Click **Options** to change the default settings for what is scanned and how to respond if a virus or security risk is detected.
The default settings are as follows:

- The default setting is to scan all files.
- For viruses, the default settings for actions are to clean the virus from an infected file and repair its effects, and quarantine the infected file if the virus cannot be removed.
- For security risks, the default settings for actions are to quarantine the security risk and remove or repair its side effects, or log the risk if it cannot be quarantined and repaired.

To apply the modified settings only to the current scan, click **OK**. To apply the settings to all future scans, click **Save Settings**.

10 Click **Advanced** to configure a scan progress dialog box to appear during the scheduled scan.

11 In the Scan Advanced Options dialog box, under Dialog options, in the drop-down list, click **Show scan progress**, and then click **OK**.

12 In the Scan Options dialog box, click **OK**.

13 In the Symantec AntiVirus main window, click **Save**.
Your computer must be turned on and Symantec AntiVirus Services must be loaded when the scan is scheduled to take place. By default, Symantec AntiVirus Services are loaded when you start your computer.
The new scan is added to the list in the Scheduled Scans folder.

About creating multiple scheduled scans

If you schedule multiple scans to occur on the same computer beginning at the same time of day, the computer may experience reduced CPU utilization, or one or more of the scheduled scans may fail to begin. For example, if you scheduled three separate scans on your computer to occur at 1:00 p.m., one scan occurring on drive C, one on drive D, and one on drive E, one or more of these scans could fail to start. In this example, a better solution is to create one scheduled scan that scans drives C, D, and E.

Creating startup scans

Some users supplement a scheduled scan with an automatic scan whenever they start their computers. Often, a startup scan is restricted to critical, high-risk folders, such as the Windows folder and folders that store Microsoft Word and Excel templates.

Note: If you create more than one startup scan, the scans will run sequentially in the order in which they were created.

Symantec AntiVirus also supplies a startup scan called the Auto-Generated Quick Scan for unmanaged clients only. This scan checks the files in memory and other common infection points on the computer for viruses and security risks each time that a user logs on to the computer. You can configure this scan in the same way that you can configure any manual scan, except that you cannot stop it from scanning the files in memory and other common infection points on the computer.

To create a startup scan

1 In Symantec AntiVirus, in the left pane, click **Startup Scans**.

2 In the right pane, click **New Startup Scan**.

3 Select one of the following types of scan to schedule:
- Quick Scan
- Full Scan
- Custom Scan

4 Click **Next**.

5 Type a name and description for the scan.

6 Click **Next**.

7 If you selected Custom Scan, then in the right pane, check the appropriate check boxes to specify where to scan.
You can check anything from the entire computer to a single file.
See "Initiating manual scans" on page 56.

8 Click **Options** to change the default settings for what is scanned and how to respond if a virus or a security risk is detected.
The default settings are as follows:
- The default setting is to scan all files.
- For viruses, the default settings for actions are to clean the virus from an infected file and repair its effects, and quarantine the infected file if the virus cannot be removed.
- For security risks, the default settings for actions are to quarantine the security risk and remove or repair its side effects, and log the risk if it cannot be quarantined and repaired.

To apply the modified settings only to the current scan, click **OK**. To apply the settings to all future scans, click **Save Settings**.

9 Click **Advanced** to configure a scan progress dialog box to appear during the startup scan.

10 In the Scan Advanced Options dialog box, under Dialog options, in the drop-down list, click **Show scan progress**, and then click **OK**.

11 In the Scan Options dialog box, click **OK**.

12 In the Symantec AntiVirus main window, click **Save**.
The scan runs every time that you start your computer and Windows loads.

Creating user-defined scans

If you regularly scan the same set of files or folders, you can create a user-defined scan that is restricted to just those items. At any time, you can quickly verify that the specified files and folders are free from viruses and security risks.

Create user-defined scans

You can create a user-defined scan that can be run manually at any time.

To create a user-defined scan

1. In Symantec AntiVirus, in the left pane, click **User-defined Scans**.
2. In the right pane, click **New User-defined Scan**.
3. Select one of the following types of scan to schedule:
   - Quick Scan
   - Full Scan
   - Custom Scan
4. Click **Next**.
5. Type a name and description for the scan.
6. Click **Next**.
7. If you selected Custom Scan, then in the right pane, check the appropriate check boxes to specify where to scan.
   You can check anything from the entire computer to a single file.
   See "Initiating manual scans" on page 56.
8. Click **Options** to change the default settings for what is scanned and how to respond if a virus or security risk is detected.
   The default settings are as follows:
   - The default setting is to scan all files.
   - For viruses, the default settings for actions are to clean the virus from an infected file and remove or repair its effects, and quarantine the infected file if the virus cannot be removed.
   - For security risks, the default settings for actions are to quarantine the security risk and remove or repair its side effects, and log the risk if it cannot be quarantined and repaired.

   To apply the modified settings only to the current scan, click **OK**. To apply the settings to all future scans, click **Save Settings**.
9. Click **Advanced** to configure a scan progress dialog box to appear during the scheduled scan.
10. In the Scan Advanced Options dialog box, under Dialog options, in the drop-down list, click **Show scan progress**, and then click **OK**.
11. In the Scan Options dialog box, click **OK**.
12. In the Symantec AntiVirus main window, click **Save**.

To run a user-defined scan

1. In Symantec AntiVirus, in the left pane, expand **User-defined Scans**.
2. Double-click the saved user-defined scan.

Editing and deleting startup, user-defined, and scheduled scans

You can reconfigure existing scans at any time. You can also delete scans, if necessary.

Edit and delete scans

You can edit and delete existing startup, user-defined, and scheduled scans. Certain options may be grayed out if they are not configurable for a particular type of scan.

To edit a scan

1. In Symantec AntiVirus, in the left pane, select the scan to edit.
2. Click **Edit**.
3. Do any of the following:
   - If it is a user-defined scan, then on the Files tab, select the files, folders, or drives to scan.
   - If it is a scheduled scan, then on the Schedule tab, select a new scan frequency, and a scan date and time.
   - On the Name/Description tab, edit the name and description of the scan.
4. If necessary, click **Options** to change any of the following scan options:
   - File types: Scan either by file extensions or file types
   - Scan enhancements: Scan program files loaded into memory, scan common infection locations, scan for traces of well-known viruses and security risks before scanning selected files and folders
   - File and folder exclusions
   - Advanced scan options: Compressed files, storage migration, and so on
   - Actions that are performed when a virus or security risk is found
   - Throttling options
   - Notifications: Detection Options allow you to construct a message to display when a virus or security risk is found. Remediation Options allow you to configure whether or not you want to be notified before remediation actions, such as stopping a service, are going to occur.
5. Click **OK** until you return to the Symantec AntiVirus main window.

To delete a scan

- In Symantec AntiVirus, in the left pane, right-click the scan to delete, and then click **Delete**.

Configuring actions for viruses and security risks

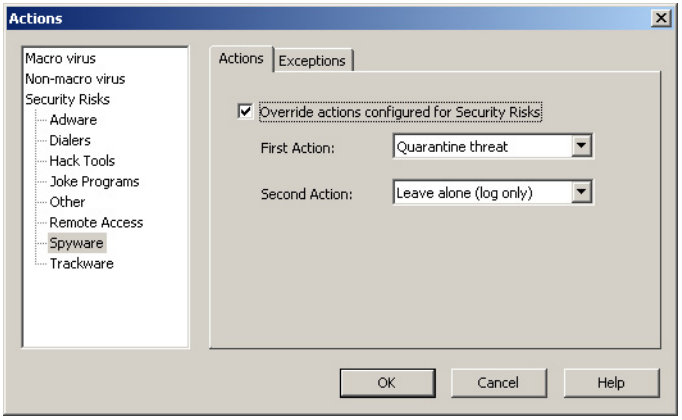
An important part of scanning for both viruses and security risks is to configure the actions that you want Symantec AntiVirus to take when it detects a virus or security risk. You can configure a first action and a second action to take if the first action fails.

Note: If an administrator manages your computer, and these options display a padlock icon, you cannot change these options because your administrator has locked them.

This procedure uses configuring a Full Scan as an example, but you can configure actions for viruses, security risk items, and categories in the same way when you configure other scans.

To configure actions for viruses and security risks

1. In the left pane, expand **Scan**, and then click **Full Scan**.
2. In the right pane, click **Options**.
3. In the Scan Options window, click **Actions**.



4 In the Actions dialog box, in the tree, select a type of virus or security risk.
By default, each security risk subcategory, such as Spyware, is automatically configured to use the actions that are set at the top level for the entire Security Risks category.
To configure a category or specific instances of a category to use different actions, check **Override actions configured for Security Risks**, and then set the actions for that category only.

5 Select a first and second action from the following options:

Clean threat	Removes the virus from the infected file. This is the default first action for viruses. **Note:** This action is not available for security risks. Cleaning should always be the first action for viruses. If Symantec AntiVirus successfully cleans a virus from a file, you don't need to take any other action. Your computer is free of viruses and is no longer susceptible to the spread of that virus into other areas of your computer. When Symantec AntiVirus cleans a file, it removes the virus from the infected file, boot sector, or partition tables, and eliminates the ability of the virus to spread. Symantec AntiVirus can usually find and clean a virus before it causes damage to your computer. In some instances, however, depending on the amount of damage that a virus has already caused, the cleaned file might not be usable. This is a result of the virus infection, and not a result of the clean action. Some infected files cannot be cleaned.
Quarantine risk	Does one of the following: ■ For viruses, moves the infected file from its original location to the Quarantine. Infected files within the Quarantine cannot spread viruses. This is the default second action for viruses. ■ For security risks, moves the infected files from their original location to the Quarantine and attempts to remove or repair any side effects. This is the default first action for security risks. Quarantine contains a record of all actions that were performed so that if needed, you can return the computer to the state that existed before Symantec Client Security removed the risk.

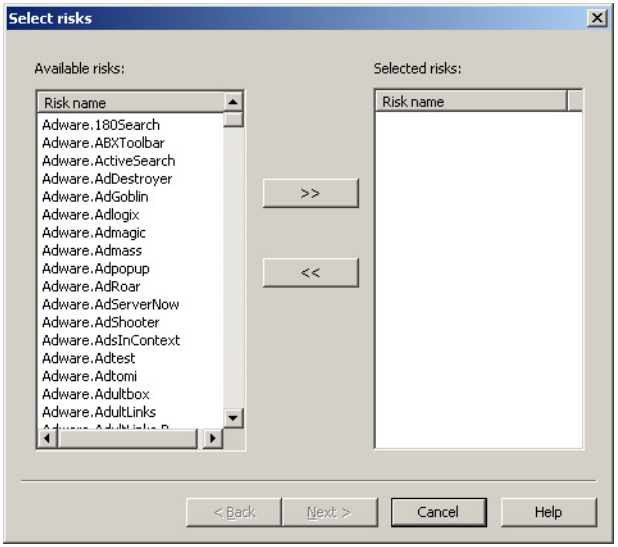
Delete risk	Deletes the infected file from your computer's hard drive. If Symantec AntiVirus cannot delete a file, additional information about the action that Symantec AntiVirus took appears in the Notification dialog box and the Event Log. Use this action only if you can replace the file with a backup copy that is free of viruses or security risks, because the file is permanently deleted and cannot be recovered from the Recycle Bin. **Note:** Use this action with caution when you configure actions for security risks, because in some cases, deleting security risks can cause applications to lose functionality.
Leave alone (log only)	Does one of the following: ■ For viruses, leaves the infected file as is. The virus remains in the file, capable of spreading the infection to other parts of your computer. An entry is placed in the Risk History to keep a record of the infected file. You can use Leave alone (log only) as a second action for both macro and non-macro viruses. Do not select this action when you perform large-scale, automated scans such as scheduled scans unless you intend to view the scan results and take an additional action later, such as moving the file to the Quarantine. ■ For security risks, leaves the infected file as is and places an entry in the Risk History to keep a record of the risk. Use this option to take manual control of how Symantec AntiVirus handles a security risk. This is the default second action for security risks. Your system administrator might send a customized message that explains how to respond.

See "Tips for assigning second actions for viruses" on page 69.
See "Tips for assigning second actions for security risks" on page 70.

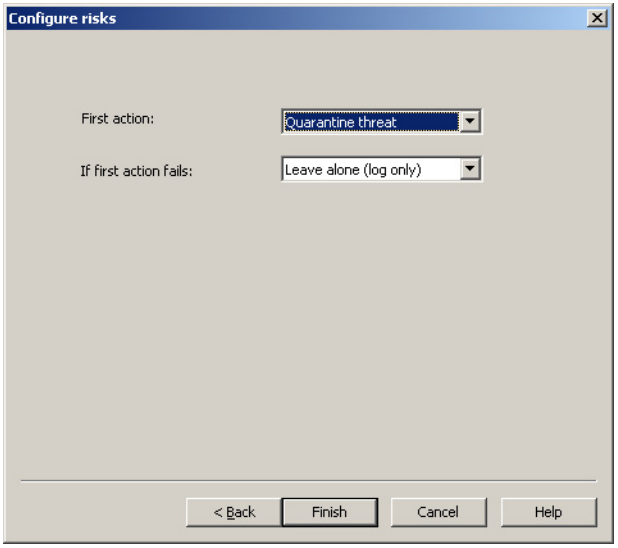
6 Repeat steps 4 and 5 for each category for which you want to set specific actions.

7 If you selected a security risk category in the tree, you can click the Exceptions tab to configure custom actions for one or more specific instances of that security risk category.

8 Click **Add**.



9 In the Select risks dialog box, in the list, select the specific risks for which you want to configure custom actions, and then click **Next**.



10 In the Configure risks dialog box, select the first and second actions that you want Symantec AntiVirus to take when it detects the risks that you selected, and then click **Finish**.

11 Repeat steps 8 through 10 for each security risk for which you want to set specific actions.

12 Click **OK** until you return to the Symantec AntiVirus main window.

Tips for assigning second actions for viruses

When you select a second action for viruses, consider the following:

- The level of control that you need to have over your files
  If you store important files on your computer without backing them up, you should not use actions like Delete threat. Though you may delete a virus this way, you could lose important data.
  Another consideration is your system files. Because some of your system files have executable extensions, they could potentially be attacked by file viruses. Though somewhat inconvenient, it's a good idea to use the Leave alone (log only) or Quarantine threat action so that you can check which files have been infected. For example, if Command.com were infected by a file virus and Symantec AntiVirus were unable to clean an infection, you might not be able to restore the file. However, using the Leave alone (log only) command could save you additional trouble caused by not restoring Command.com before turning off your computer.
- The type of virus that has infected your computer
  Different types of viruses target different areas of your computer for infection. Boot viruses infect boot sectors, partition tables, master boot records, and sometimes memory. When boot viruses are multipartite, they may also infect executable files, and the infection can be treated similarly to a file virus. File viruses typically infect executable files that have .exe, .com, or .dll extensions. Macro viruses infect document files and macros associated with those documents. Select actions based on the types of files that you might need to recover.
- The type of scan that is being performed
  All scans perform actions automatically without your consent. If you do not change the actions before a scan, the default actions are used. As a result, the default second actions are designed to give you control of a virus outbreak situation. For scans that work automatically such as scheduled scans, idle scans (on 32-bit computers), and Auto-Protect scans, do not assign second actions that have permanent effects. For example, limit the Delete threat and Clean threat or Delete threat actions to a manual scan that you perform when you already know that a file is infected.

Tips for assigning second actions for security risks

When you select a second action for security risks, consider the level of control that you need to have over your files. If you store important files on your computer without backing them up, you should not use the Delete risk action. Though you might delete a security risk this way, you could potentially cause another application on your computer to stop working. Use the Quarantine risk action instead so that you can reverse the changes that Symantec AntiVirus makes, if necessary.

Configuring notifications for viruses and security risks

By default, you are notified when a Symantec Client Security scan find a virus or security risk. By default, you are also notified when Symantec Client Security needs to terminate services or stop processes to remove or repair the effects of virus or security risk.

You can configure the following notifications for scans:

Detection Options	Construct the message that you want to appear when Symantec Client Security finds a virus or a security risk on your computer. If you are configuring File System Auto-Protect, you can select an additional option to display a dialog box that contains the results when Auto-Protect finds viruses and security risks on your computer.
Remediation Options	Configure whether or not you want to be notified when Symantec AntiVirus finds a virus or a security risk, and needs to terminate a process or stop a service to finish removing or repairing a risk.

You can construct the detection message that you want to appear on your computer by typing directly in the message field to add your own text, and you can right-click in the message field to select variables.

Table 3-2 describes the variable fields that are available for notifications messages.

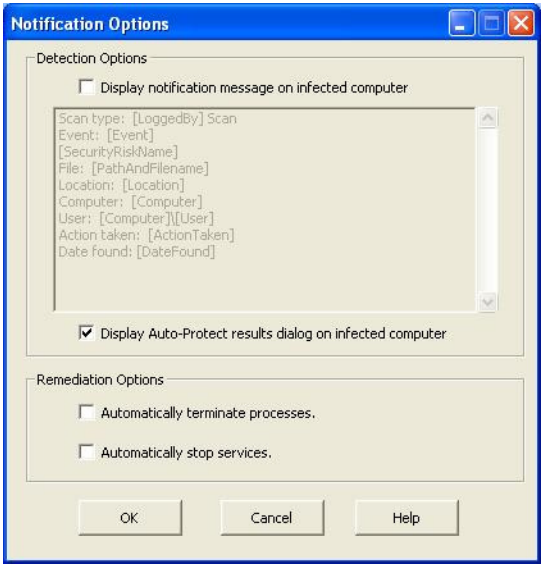
Table 3-2 Notifications message variable fields

Field	Description
VirusName	The name of the virus or security risk that was found.
ActionTaken	The action that was taken in response to detecting the virus or security risk. This can be either the first action or second action that was configured.
Status	The state of the file: Infected, Not Infected, or Deleted. This message variable is not used by default. To display this information, manually add this variable to the message.
Filename	The name of the file that the virus or security risk infected.
PathAndFilename	The complete path and name of the file that the virus or security risk infected.
Location	The drive on the computer on which the virus or security risk was located.
Computer	The name of the computer on which the virus or security risk was found.
User	The name of the user who was logged on when the virus or security risk occurred.
Event	The type of event, such as “Risk Found.”
LoggedBy	The type of scan, manual, scheduled, and so on, that detected the virus or security risk.
DateFound	The date on which the virus or security risk was found.
StorageName	The affected area of the application, for example, File System Auto-Protect or Lotus Notes Auto-Protect.
ActionDescription	A full description of the actions that were taken in response to detecting the virus or security risk.

This procedure uses configuring a Full Scan as an example, but you can also configure notifications in the same way when you configure other scans.

To configure notifications for viruses and security risks

1. In the left pane, expand **Scan**, and then click **Full Scan**.
2. In the right pane, click **Options**.
3. In the Scan Options window, click **Notifications**.



4. In the Notifications Options window, under Detection Options, check **Display notification message on infected computer** if you want a message to appear on your computer when the scan finds a virus or security risk.
5. In the message box, do any or all of the following to construct the message that you want:
   - Click to type or edit text.
   - Right-click, click **Insert Field**, and then select the variable field that you want to insert.
   - Right-click, and then select Cut, Copy, Paste, Clear, or Undo.
6. If you are configuring notifications for File System Auto-Protect, then under the message box, there is an extra option. Uncheck **Display Auto-Protect results dialog on infected computer** if you want to suppress the dialog box that contains results when Auto-Protect finds viruses and security risks.

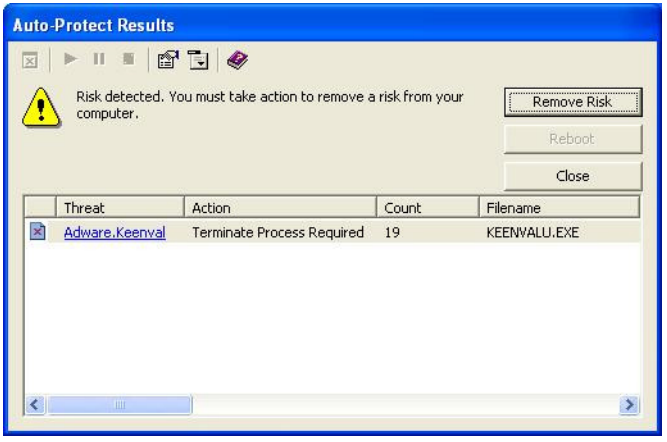
7 Under Remediation Options, check the options that you want to set. Your options are as follows:

Automatically terminate processes	If checked, Symantec Client Security automatically terminates processes when it needs to do so to remove or repair a virus or security risk. You will not be prompted to save data before Symantec Client Security terminates the processes.
Automatically stop services	If checked, Symantec Client Security automatically stops services when it needs to do so to remove or repair a virus or security risk. You will not be prompted to save data before Symantec Client Security stops the services.

8 Click **OK** until you return to the Symantec AntiVirus main window, and then click **Scan**.

Interaction with notifications

If you leave the defaults, then you are notified when Symantec Client Security finds a virus or a security risk. The Auto-Protect Results dialog box appears:



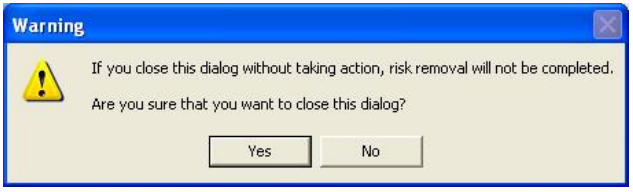
If Symantec Client Security needs to terminate a process or application or stop a service, the Remove Risk button is active. When you click Remove Risk, the following message appears:

This gives you the opportunity to save your work and close open applications, if you haven't already done so. After saving your data, you can return to this message box and click Yes to complete the removal or repair.

If Symantec Client Security needs to restart the computer to complete the removal or repair, the Reboot button is active. When you click Reboot, the following message appears:

This gives you the opportunity to save your work and close open applications, if you haven't already done so. After saving your data, you can return to this message box and click Yes to restart your computer. If you click No and close the message box without restarting, the removal or repair will not be complete until you restart your computer the next time.

And finally, if you opt to close the message box without taking an action needed to complete the removal or repair, the following message appears:



If you click Yes and closes the dialog without taking any action, the risk can be removed or repaired at a later time in the following ways:

- You can open the Risk History, right-click the risk, and then take an action.
- You can run a scan to redetect the risk and reopen the results dialog box.

The actions that can be taken depend on the actions that were configured for the particular type of virus or security risk that was found.

If you click No, you are returned to the results dialog box so that you can take the appropriate action.

Interpreting scan results

Whenever a manual, scheduled, startup, or user-defined scan runs, Symantec AntiVirus can display a scan progress dialog box to report progress, but you must configure it to do so.

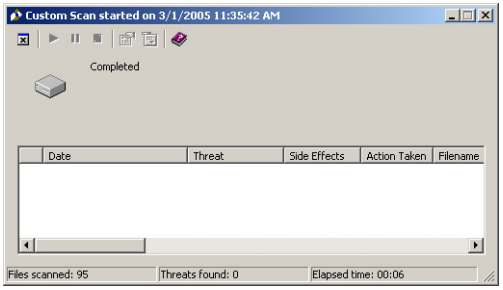
See "Initiating manual scans" on page 56.

See "Creating scheduled scans" on page 59.

See "Creating startup scans" on page 61.

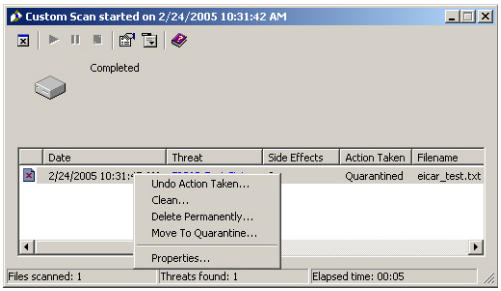
See "Creating user-defined scans" on page 62.

If you configure Symantec AntiVirus to display a scan progress dialog box, you can pause, restart, or stop the scan. When the scan is completed, results appear in the list. If no viruses or security risks are detected, the list remains empty and the status is completed.



If viruses or security risks are detected during the scan, the scan progress dialog box includes the names of the infected files, the names of the viruses or security

risks, and the actions taken. By default, you are notified whenever a virus or security risk is detected.



See "Acting on infected files" on page 79.

Note: In a centrally managed network, the scan progress dialog box may not appear for administrator-initiated scans. Similarly, your administrator may choose not to display alerts when a virus or security risk is detected.

Excluding files from scans

Rarely, a file that does not contain a virus is detected as infected. This might happen because a particular virus definition is designed to catch every possible variation of the virus. Because the virus definition must be necessarily broad, Symantec AntiVirus sometimes reports that a clean file is infected.

If Symantec AntiVirus continues to report a clean file as infected, you can exclude the file from scans. Exclusions are items that you don't want or need to include in scans.

You can also exclude folders if they contain software that can be detected as a security risk, such as adware, and your corporate security policy allows you to run the software.

See "About security risks" on page 18.

Set exclusions separately for each type of scan: Auto-Protect, startup, user-defined, scheduled, or manual, including Custom Scan, Quick Scan, or a Full Scan. The procedure, however, is the same.

Warning: Be careful with exclusions. If you exclude a file from a scan, no action will be taken to clean it if the file later becomes infected. This could be a potential risk to the security of your computer.

To exclude a file from a scan

1. In Symantec AntiVirus, do one of the following:
   - For Auto-Protect of the file system, in the left pane, click **Configure**, and then, in the right pane, click **File System Auto-Protect**.
   - For all other scan types, in the pane where you specify what to scan, click **Options**.
2. In the right pane or Scan Options dialog, check the exclude files and folders option.
3. Click **Exclusions**, and then click **Files/Folders** to select the file to exclude.
4. Click **OK**.
5. Click **Extensions**.
6. Specify the file types that you want to exclude, and then click **OK**.
   You can use the ? wildcard character to specify any character. For example, XL? excludes .xls, .xlt, .xlw, and .xla files.
7. Click **OK** until you return to the Symantec AntiVirus main window.

Chapter 4

What to do if a virus or security risk is found

This chapter includes the following topics:

Acting on infected files

The Symantec AntiVirus preset options for Auto-Protect and all scan types are to clean a virus from an infected file on detection, but to place the file in the Quarantine if it cannot be cleaned. For security risks, the default is to quarantine the infected files and remove or repair their side effects, and to log the detection if it cannot be repaired.

If a virus-infected file is repaired, you don't need to take further action to protect your computer. If a security risk-infected file is quarantined and removed or repaired, you don't need to take further action to protect your computer.

You can deal immediately with infected files from the scan progress dialog box once a scan completes. For example, you may decide to delete a cleaned file because you'd rather replace it with an original file.

You can act on a file that has been infected by a virus or a security risk at a later point from the Risk History or from the Quarantine.

See "Rescanning files in the Quarantine for viruses" on page 83.

Note: In a centrally managed network, the scan progress dialog box may not appear for administrator-initiated scans. Similarly, your administrator may choose not to display alerts when a virus or security risk is detected.

To act on an infected file

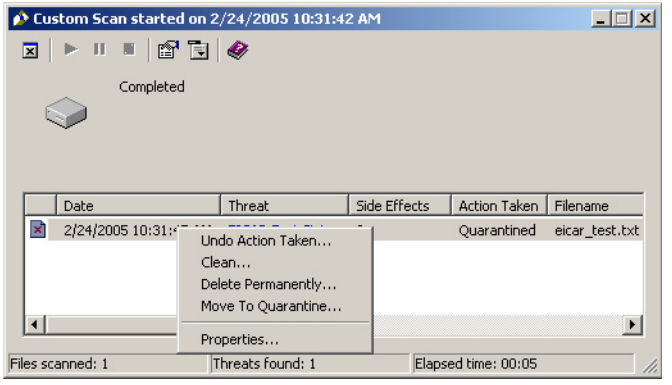
1 Do one of the following:

- In the scan progress dialog box, select the files that you want when the scan completes.
- In Symantec AntiVirus, in the left pane, expand **Histories**, click **Risk History**, and then, in the right pane, select the files you want.

2 Right-click the file or files, and then select one of the following:

- Undo Action Taken: If possible, reverses the preset action response.
- Clean (viruses only): Removes the virus from the file.
- Delete Permanently: Deletes the infected file and all side effects.
  For security risks, use this action with caution because in some cases, deleting security risks can an application to lose functionality.
- Move To Quarantine: Places the infected files in the Quarantine and for security risks, also attempts to remove or repair the side effects.
- Properties: Displays information about the virus or security risk.

Depending on the preset action for a virus or security risk detection, Symantec AntiVirus might not be able to perform the action you selected.



About damage that viruses cause

If an infection is found soon after the file became infected, the formerly infected file will probably be fully functional. In some instances, however, Symantec AntiVirus may clean an infected file that has already been damaged by the virus. For example, if Symantec AntiVirus finds the Word.Wazzu macro virus in an infected document file, Symantec AntiVirus removes the virus, but does not remove the word wazzu that the virus places in the infected document. In this case, Symantec AntiVirus cannot repair the damage that has been done to the infected file.

About the Quarantine

Sometimes Symantec AntiVirus detects an unknown virus that can't be eliminated with the current set of virus definitions, or you have a file that you think is infected but is not being detected. The Quarantine safely isolates potentially infected files on your computer. A virus in a quarantined item cannot spread.

Move files that are infected by viruses to the Quarantine

Moving a virus-infected file to the Quarantine drastically reduces the opportunity for the virus to copy itself and thus infect other files. This action is a recommended second action for both macro and non-macro virus infections.

Moving a virus-infected file to the Quarantine prevents the spread of the virus. However, it does not clean the virus, so the virus stays on your computer until the virus is cleaned or the file is deleted. Moving an infected file to the Quarantine is a useful action to perform on files that have been infected by file viruses and macro viruses, but is not useful for boot virus infections. Usually, boot viruses reside in the boot sector or partition tables of a computer; these items cannot be moved to the Quarantine.

See "About the master boot record" on page 17.

See "Boot viruses" on page 16.

After a file is moved to the Quarantine, you can attempt to clean the file, delete the file permanently, or restore it back to its original location. You can also view properties of the infected file. When virus definitions files are updated, you can rescan the virus-infected file in the Quarantine.

See "Rescanning files in the Quarantine for viruses" on page 83.

Leave files that are infected by security risks in the Quarantine

You can leave files that are quarantined because of security risks in the Quarantine or you can delete them. You should leave them in the Quarantine until you are sure that the applications on your computer have not lost any functionality.

Delete files that are infected by viruses in the Quarantine

If you delete a file in Quarantine, Symantec AntiVirus permanently deletes it from your computer's hard disk.

Deleting a file that is infected by a virus reduces the threat that a virus might spread by removing the file (and thus the virus) from your computer. Deleting the infected file is useful for file viruses and macro viruses.

Because viruses can damage parts of a file, deleting the infected file and replacing it with a clean backup file may be better than cleaning the infected file.

You can perform this action manually after an infected file has been moved into the Quarantine. Deleting the infected file in the Quarantine would be a useful way to remove a virus from a disposable file that was unable to be cleaned.

Warning: Use this option only if you have clean backups of files that you've decided to scan. You should not use this as a primary action for files that are scanned during Auto-Protect or scheduled scans.

Delete files that are infected by security risks in the Quarantine

If you delete files that are associated with a security risk, an application on your computer might not function properly if the application depends on the associated files that you deleted. Quarantine is a safer option because it is reversible. You can restore the files if any of the applications on your computer lose functionality after you quarantine the dependent program files.

Note: Once you have run the application that was associated with the security risk and are sure that there is no loss of functionality, you might want to delete the files to save disk space.

Managing the Quarantine

You can place files that are infected by viruses or security risks in the Quarantine.

Files are placed in the Quarantine in one of two ways:

- Symantec AntiVirus is configured to move infected items detected during Auto-Protect or a scan to the Quarantine.
- You manually select a file and add it to the Quarantine.

The Symantec AntiVirus preset options for Auto-Protect and all scan types are to clean a virus from an infected file on detection, but to place the file in the Quarantine if it cannot be cleaned. For security risks, the default option is to place the infected files in the Quarantine, and to repair the side effects of the security risk.

To add a file manually to the Quarantine

1. In Symantec AntiVirus, in the left pane, click **View**.
2. In the right pane, click **Quarantine**.
3. On the toolbar, click **Add New Item to Quarantine**.
4. Locate and select the file, and then click **Add**.
5. Click **Close**.

Viewing files and file details in the Quarantine

You can view files that have been placed in the Quarantine and details about the files, such as the name of the virus, the name of the computer on which the file was found, and so on.

To view files and file details in the Quarantine

1. In Symantec AntiVirus, on the View menu, click **Quarantine**.
2. Right-click the file that you want to view, and then click **Properties**.

Rescanning files in the Quarantine for viruses

If a file is placed in the Quarantine, update your definitions. Depending on how your administrator has configured the Quarantine, when definitions have been updated, files in the Quarantine might get scanned, cleaned, and restored automatically or the Repair Wizard might appear, letting you rescan the files in the Quarantine.

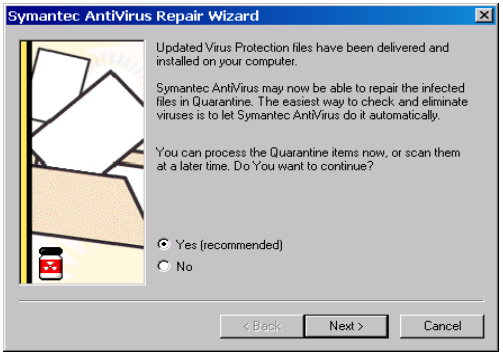
If, after Symantec AntiVirus rescans the file in the Quarantine, it still can't remove the virus, you can submit the infected file to Symantec Security Response for analysis.

See "Submitting a potentially infected file to Symantec Security Response for analysis" on page 87.

To rescan files in the Quarantine using the Repair Wizard

1 If the Repair Wizard appears, click **Yes**.

2 Click **Next** and follow the on-screen instructions to rescan the files in the Quarantine.



Rescanning files manually

You can manually rescan a file in the Quarantine for viruses, but not for security risks.

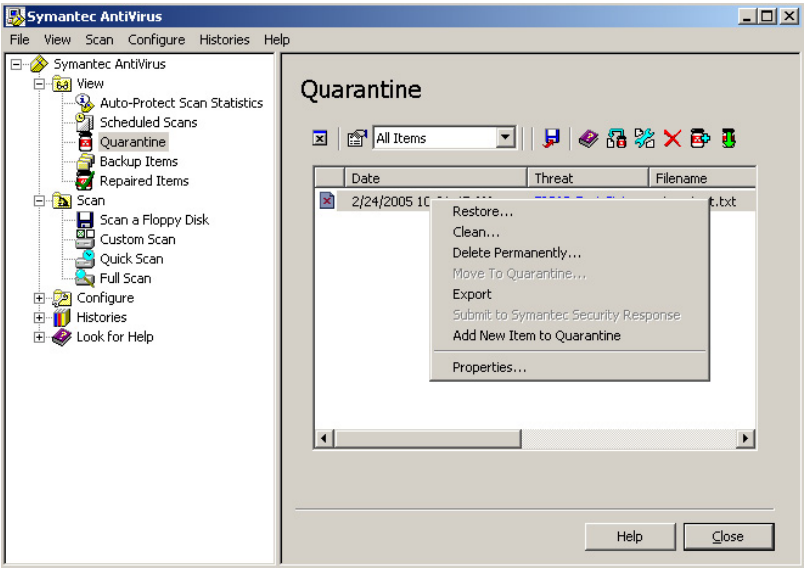
To rescan a file in the Quarantine manually for viruses

1 Update your definitions.
See "Keeping virus and security risk protection current" on page 37.

2 In Symantec AntiVirus, in the left pane, click **View**.

3 In the right pane, click **Quarantine**.

4 Select the file in the Quarantine listing.



5 Do one of the following:

- Right-click the file, and then click **Clean**.
- In the right pane on the toolbar, click **Clean**.

6 Click **Start Clean**.

The file is scanned again with the new definitions and replaced in its original location.

When a repaired file can't be returned to its original location

Occasionally, a clean file does not have a location to which to be returned. For example, an infected attachment may have been stripped from an email and placed in the Quarantine. In this special circumstance, the cleaned file is placed in Repaired Items instead. You must release the file and specify a location.

To release a cleaned file from Repaired Items

1 In Symantec AntiVirus, in the left pane, click **View**.

2 In the right pane, click **Repaired Items**.

3 Right-click the file, and then click **Restore**.

4 Specify the location for the cleaned file.

Clearing Backup Items

As a data safety precaution, by default Symantec AntiVirus is configured to make backup copies of items that are infected by viruses and security risks before attempting a clean or a repair. After an item has been successfully cleaned of a virus, you should manually delete it from Backup Items because the backup is still infected. You can also set up a time period in which files are deleted automatically.

See "Automatically purging files from the Quarantine, Backup Items, and Repaired Items" on page 87.

To manually clear Backup Items

1. In Symantec AntiVirus, in the left pane, click **View**.
2. In the right pane, click **Backup Items**.
3. Select one or more files in the Backup Items listing.
4. Do one of the following:
   - Right-click the file, and then click **Delete Permanently**.
   - In the right pane on the toolbar, click **Delete**.
5. In the Take Action dialog box, click **Start Delete**.
6. Click **Close**.

Deleting files from the Quarantine

You can manually delete files that you no longer need from the Quarantine. You can also set up a time period by which files are deleted automatically.

See "Automatically purging files from the Quarantine, Backup Items, and Repaired Items" on page 87.

Note: Your administrator may specify a maximum number of days that items are allowed to stay in the Quarantine. Items are automatically deleted from the Quarantine after that time limit.

To manually delete files from the Quarantine

1. In Symantec AntiVirus, in the left pane, click **View**.
2. In the right pane, click **Quarantine**.
3. Select one or more files in the list of quarantined items.
4. Right-click the files, and then click **Delete Permanently**.

5 In the Take Action dialog box, click **Start Delete**.

6 Click **Close**.

Automatically purging files from the Quarantine, Backup Items, and Repaired Items

You can set up Symantec AntiVirus to automatically remove items after a specified time interval from the Quarantine, Backup Items, and Repaired Items. This prevents the buildup of files that you may forget to remove manually from these areas.

To automatically purge files

1 In Symantec AntiVirus, in the left pane, click **View**.

2 In the right pane, select one of the following:

- Quarantine
- Backup Items
- Repaired Items

3 Click the Purge icon on the far right of the toolbar.

4 In the Purge Options dialog box, check **Enable automatic files purging**.

5 In the Purge after text box, type a number or click an arrow to select a number.

6 Select the time period interval.

7 Click **OK**.

Submitting a potentially infected file to Symantec Security Response for analysis

Sometimes, Symantec AntiVirus cannot clean a virus from a file. Or, you suspect that a file is infected and is not being detected. If you submit the file to Symantec Security Response, they can analyze your file to make sure that it is not infected. You must have an Internet connection to submit a sample.

Note: In a centrally managed network, submissions to Symantec Security Response are usually handled by your administrator from the Symantec Central Quarantine. In this case, the Submit to Symantec Security Response option is not available in your version of Symantec AntiVirus. Also, the Submit to Symantec Security Response option is not available if the administrator configures an unmanaged client to not allow submissions to Symantec Security Response.

To submit a file to Symantec Security Response from the Quarantine

1. In Symantec AntiVirus, in the left pane, click **View**.
2. In the right pane, click **Quarantine**.
3. Select the file in the list of quarantined items.
4. In the right pane on the toolbar, click **Submit To Symantec Security Response**.
5. Follow the on-screen instructions in the wizard to collect the necessary information and submit the file for analysis.

Viewing the Event Log

The Event Log contains daily records of virus and security risk activities that are related to protection on your computer, including configuration changes, errors, and virus and security risk definitions file information. These records, called events, are displayed with additional relevant information in a list format.

By using the information in the Event Log, you can track trends that are related to viruses and security risks on your computer. If your computer is used by several people, you might be able to identify who is introducing the most viruses or security risks, and help that person to use better precautions.

To view the Event Log

- In Symantec AntiVirus, on the Histories menu, click **Event Log**.

Filtering items in the Event Log

You can filter events in the Event Log by Date, Event, Computer, User, or Scan Type that logged the event. You can also filter by date or by categories of events, so that you can view information for a few days or information for the last few years.

Filtering items by date

You can filter items that appear in the Risk History, Scan History, Event Log, and Tamper History by date.

By default, Symantec AntiVirus enters events in the Event Log in the order in which the events happen. All of the events that occurred on your computer since Symantec AntiVirus was installed are stored.

When you change the date range, Symantec AntiVirus does not delete the information. For example, if you change the information that appears to Today, the other information continues to exist, but does not appear in the history or log.

To filter items by date

1. On the Histories menu, click **Event Log**.
2. Click the **All Items** (or date range) drop-down list box.
3. Select a filter.
4. If you clicked Selected range, select a start date and an end date, and then click **OK**.

Filtering the Event Log by event category

After you have displayed the information that you want to view in the Event Log, you can save the data as it is displayed on your computer to a comma-separated value (.csv) file.

Events are divided into the following categories in the Event Log:

- Configuration change
- Symantec AntiVirus startup/shutdown
- Virus definition file
- Scan omissions
- Forward to Quarantine Server
- Deliver to Symantec Security Response
- Auto-Protect load/unload
- Licensing
- Client management and roaming
- Log Forwarding

- Unauthorized communication (access denied) warnings
- Login and certificate management

You can reduce the number of events that appear in the Event Log by displaying only certain categories of events.

For example, if you wanted to view only error events, you could select only the Configuration Change category. While Symantec AntiVirus would continue to record events in the other categories, those events would not appear in the Event Log.

To filter the Event Log by event category

1. In Symantec AntiVirus, on the Histories menu, click **Event Log**.
2. Click **Filter Event Log**.
3. Select one or more categories of events.
4. Click **OK**.

About clearing items from the Event Log

You cannot permanently remove event records from the Event Log from within Symantec AntiVirus.

To permanently delete Event Log records, you must delete the .log files that contain the event records. Events are recorded in .log files for each day of the week in the Symantec AntiVirus Logs directory. These files are named according to the day that they were created. Deleting .log files is not recommended, because you will permanently lose the historical virus protection data that is contained in them.

Exporting data to a .csv file

You can export information into comma-separated value (.csv) format. This common file format is used by most spreadsheet and database programs to import data. Once in another program, you can use the data to create presentations, graphs, or combine the data with other information to create complex reports.

You can export only the data that is displayed. For example, if you changed Symantec AntiVirus settings to show information for the last seven days, only information for the last seven days would appear in the .csv file.

To export data to a .csv file

1. In the Risk History, Scan History, or Event Log window, make sure that the data that you want to save is displayed.
2. Click **Export**.
3. In the Save As dialog box, locate the directory in which you want to save the file, and then type a file name.
4. Click **Save**.

Section 2

Symantec Client Firewall

Chapter 5

Introducing Symantec Client Firewall

This chapter includes the following topics:

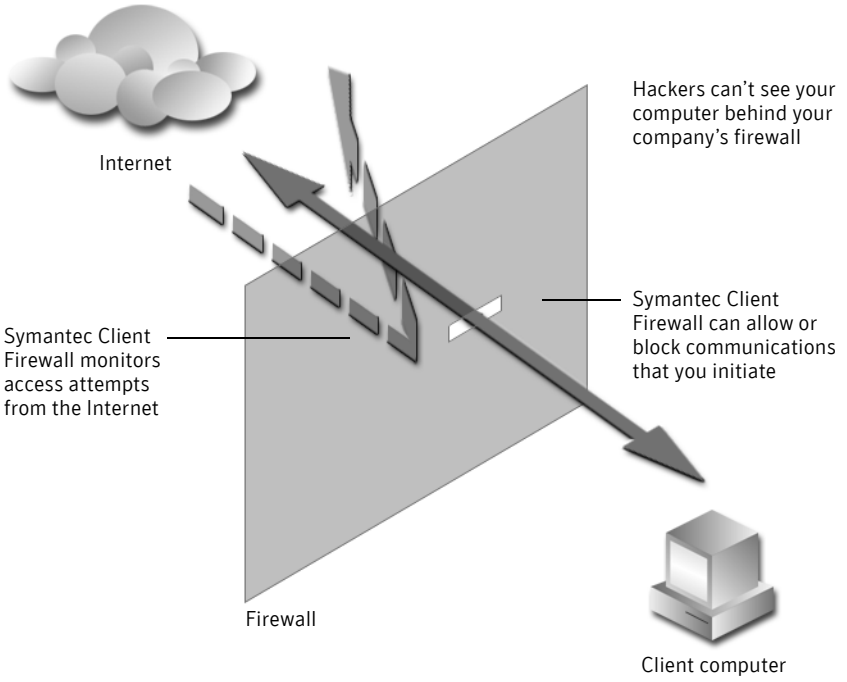
What's new in Symantec Client Firewall

Symantec Client Firewall now includes the following features:

Protocol Filtering	Lets you permit or block IP traffic that uses less common Internet Protocol (IP) protocols that Symantec Client Firewall previously permitted unconditionally. See "Using Protocol Filtering" on page 155.
User Permissions	Determines your level of interaction with Symantec Client Firewall. See "About Symantec Client Firewall permissions" on page 103.
Intrusion Prevention improvements	Better protects client computers from intrusion attempts by using new Intrusion Prevention technology. Intrusion Prevention now includes smarter detection signatures, and a stateful engine that remembers network traffic patterns and applies this information to subsequent traffic inspections. See "How Intrusion Prevention analyzes traffic" on page 131.
Privacy Control	Blocks private information from Web sites, in email, and in instant messages (enhanced version). See "About protecting your privacy" on page 165.
Statistics	Lets you view details of the recent attacks on your computer and the actions that were taken on cookies, private information, and Ad Blocking (enhanced version). See "Viewing the Statistics window" on page 186.
Log Viewer	Lets you view details of the actions that Symantec Client Firewall takes to protect your computer. You can now choose between default and verbose logging levels. See "About the logging level" on page 191.
Intrusion Prevention signature alerts	Lets you exclude individual Intrusion Prevention signatures from alerting you when they are triggered See "Excluding Intrusion Prevention alerts" on page 158.
Protection Alert	Gives you the option to temporarily disable Symantec Client Firewall, the Client Firewall component, and Intrusion Prevention. See "Disabling Symantec Client Firewall temporarily" on page 110.

About Symantec Client Firewall

Symantec Client Firewall protects computers from hackers, protects your privacy, and eliminates unwanted sources of network traffic.



Symantec Client Firewall provides a barrier between your computer and the Internet. A firewall prevents unauthorized users from accessing privately owned computers and networks connected to the Internet.

Symantec Client Firewall prevents unauthorized access to your computer when you are on the Internet, detects possible hacker attacks, protects your personal information, and eliminates unwanted sources of network traffic.

Symantec Client Firewall and Symantec Client Security

Symantec Client Firewall is a component of Symantec Client Security. At the client level, Symantec Client Security includes the following forms of protection:

- Virus protection
- Expanded threat detection and repair
- Content filtering
- Firewall
- Intrusion Prevention

These forms of protection keep the network safe at the client level by identifying and removing blended threats. Blended threats use multiple methods of attack including worms, email and application vulnerabilities, and network shares to gain control of systems. Code Red and Nimda are examples of blended threats.

Note: Symantec Client Firewall and the Intrusion Prevention engine do not support 64-bit platforms in this release. Check the Release Notes and Readme that accompany each new release for updates on 64-bit support.

Symantec Client Firewall features

Symantec Client Firewall includes a number of security tools that help keep your computer safe. Internet security can be a complicated topic to understand, so Symantec Client Firewall includes the Alert Assistant, which helps you understand security issues, suggests how you can resolve problems, and advises you on avoiding future security problems.

Table 5-1 lists the features that are available in Symantec Client Firewall.

Table 5-1 Symantec Client Firewall features

Feature	Description
Stateful inspection	Tracks information about current connections such as source and destination IP addresses, ports, applications, and so forth. Ensures that inbound traffic is a legitimate reply to outbound traffic, and enables rulebase simplification. See "About stateful inspection" on page 146.
Internet status	Provides a snapshot of your computer's network activity that you can use to identify ongoing attack attempts and review how program settings affect your protection. See "About monitoring Symantec Client Firewall" on page 185.
Client Firewall	Protects your computer from Internet hackers and unauthorized intrusions. Makes your computer virtually invisible to others on the Internet. Protects remote and mobile users from hacker attacks and prevents these systems from being used by hackers to gain back-door access to the corporate network. See "How Symantec Client Firewall protects against network attacks" on page 130.
Intrusion Prevention	Detects and blocks malicious traffic and attempts by outside users to attack your computer. Intrusion Prevention also monitors outbound traffic and prevents the spread of worms. See "How Symantec Client Firewall protects against network attacks" on page 130.
Privacy Control	Gives you several levels of control over the kinds of information that users, Web browsers, instant messenger programs, and email clients can send over the Internet. See "About protecting your privacy" on page 165.
Ad Blocking	Speeds up your Web surfing by eliminating banner ads and other slow-loading or intrusive content. Symantec Client Firewall now also blocks ads made with Macromedia® Flash® and prevents sites from opening pop-up or pop-under ad windows. See "Blocking ads" on page 173.

Table 5-1 Symantec Client Firewall features

Feature	Description
Location Awareness	Lets you implement specific sets of rules and Zones based on the network access point used to connect to the Internet. See "Using Location Awareness" on page 117.
Secure Port	Secures the ports defined in Trojan rules so completely that traffic destined for these ports, both inbound and outbound, never triggers firewall rulebase inspection. Programs that use random ports will not attempt to use the secured ports. See "Using Secure Port" on page 152.
Protocol Filtering	Lets you selectively permit or block all IP protocols to Symantec Client Firewall for increased security, instead of being limited to configure TCP, UDP, ICMP, and IGMP protocols. Virtual Private Networks (VPN) and IP multicasting use less common protocols that you can configure by using Protocol Filtering.
Settings Manager	Lets you export and import policy files to provide backup and restore functionality. See "Exporting and importing policy files" on page 108.
VPN support	Lets Symantec Client Firewall work with the following VPNs: ■ Check Point® ■ Nortel Contivity® ■ Microsoft ■ iPass® ■ Fiberlink® With most VPNs, when the VPN client is active, you cannot see the Internet or other computers on your local network. You can see only what is available through the VPN server to which you are connected. Ad Blocking and Privacy Control are not supported over encrypted connections.

Chapter 6

Symantec Client Firewall basics

This chapter includes the following topics:

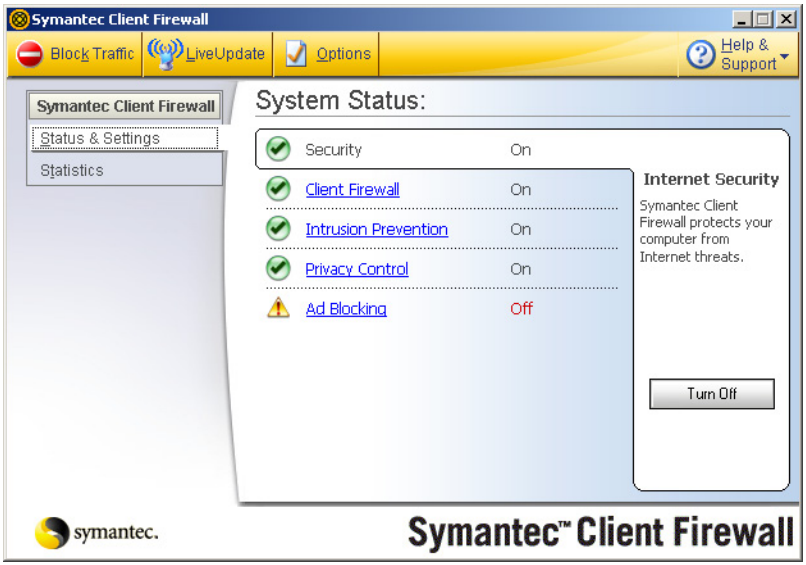
Accessing Symantec Client Firewall

After installation, Symantec Client Firewall automatically protects any computer on which it is installed. You do not have to start the program to be protected.

To access Symantec Client Firewall

- Do one of the following:
  - In the Windows system tray, double-click the Symantec Client Firewall icon.

- On the Windows taskbar, click **Start** > **Programs** > **Symantec Client Security** > **Symantec Client Firewall**.



Displaying the Symantec Client Firewall system tray menu

Symantec Client Firewall adds an icon to the Windows system tray. By default, the Symantec Client Firewall system tray icon appears in the lower-right corner of your computer monitor. Right-click this icon to open a menu that contains frequently used Symantec Client Firewall tools.

Note: The Symantec Client Firewall Options window allows you to override the default setting and hide the system tray icon for Symantec Client Firewall. Additionally, the window contains configurable settings to hide the Log Viewer and View Statistics menu options.

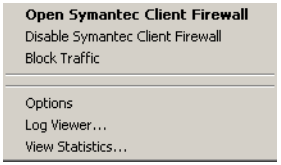
On the system tray menu, you have the following options:

- Open the Symantec Client Firewall main window.
- Enable and disable Symantec Client Firewall.
- Block or permit traffic to and from your computer.
- Display the Options window.

- Display the Log Viewer.
- Display the Statistics window.

To display the Symantec Client Firewall system tray menu

- Right-click the icon.



Working with Symantec Client Firewall

Symantec Client Firewall works in the background. Your system administrator determines the level of interaction that you have with the program by permitting or blocking your ability to configure firewall features and options. Depending on the permissions that your system administrator gives you, you might interact with the program only when it alerts you of new network connections and possible problems, or you might have full access to the user interface. When you have full access, you can control the number of alerts that you receive and how the program resolves potential security problems.

About Symantec Client Firewall permissions

Your permissions determine which Symantec Client Firewall features you can view and use. Your system administrator defines your permissions. Each firewall feature or option is tied to a permission setting.

Depending on your permissions, you might not have access to the user interface, you might have access to configure all firewall options, or you might be limited to perform specific tasks that require user input, such as configuring rules for certain Internet traffic. There are some dependencies among permissions. For example, if you have permissions to create and modify firewall rules, but do not have permissions to access the Symantec Client Firewall user interface, you cannot configure rules because you do not have access to the rules dialog box. Features that you cannot configure are removed from or appear dimmed in the Symantec Client Firewall user interface.

Changing settings for Symantec Client Firewall protection features

The default settings for Symantec Client Firewall provide a safe, automatic, and efficient way of protecting your computer. If you want to change or customize your protection, you can access many Symantec Client Firewall tools in the Status & Settings window.

To change settings for Symantec Client Firewall protection features

1. In the main window, click **Status & Settings**.
2. Double-click a feature that you want to customize.
3. Configure the feature.
4. When you finish making changes, click **OK**.

Responding to Symantec Client Firewall alerts

Symantec Client Firewall monitors communication activities to and from your computer and lets you know when an activity that may compromise your security is taking place.

Symantec Client Firewall shows the following types of alerts:

- Security
- ActiveX®
- Privacy Control
- Cookie
- Intrusion Prevention
- Internet Protocol
- Java™
- Listen
- Launcher
- Module finger printing
- Service Monitor
- Location Awareness
- DNS
- Trojan horse

When an alert appears, read it before you make a decision. Identify what type of alert it is and the threat level. Once you understand the risks, you can make a

choice. Take as much time as you need to make your choice. Your computer is safe from attack while the alert is active.

Symantec Client Firewall helps you decide on an appropriate action by selecting the recommended action if one exists. Symantec Client Firewall cannot suggest recommended actions for all alerts.

Not every Security Alert represents an attempt to attack your computer. There are many harmless events that occur on the Internet that cause Security Alerts. Some alerts allow you to select not to see these alerts again.

Using the Alert Assistant

Each Symantec Client Firewall alert includes a link to the Alert Assistant. The Alert Assistant includes the following customized information about each alert:

- The type of alert
- The communication that triggered this alert
- Additional information
- What you should do
- How to reduce the number of these alerts that you receive

To use the Alert Assistant

1. In any alert window, click the **Alert Assistant** link.
2. In the Alert Assistant window, review the information about this alert.
3. To respond to the alert, close the Alert Assistant.

Stopping Internet communication with Block Traffic

Symantec Client Firewall includes a Block Traffic button that lets you immediately halt any communication between your computer and another. This can help limit any damage to your computer if it is attacked, if a Trojan horse is sending personal information without your permission, or if you inadvertently allow an untrusted person to access files on your computer.

When this option is active, Symantec Client Firewall stops all communication to and from your computer. To the outside world, it appears that your computer has completely disconnected from the Internet.

If you want to block all traffic into and out of your computer, Block Traffic is more effective than simply using your Internet software to disconnect. Most Internet programs can automatically connect without any input from the user, so a malicious program could reconnect when you are away from the computer.

Note: Block Traffic is meant to be used as a temporary measure while you address a security problem. If you restart your computer, Symantec Client Firewall automatically allows all incoming and outgoing communication.

To stop Internet communication with Block Traffic

1. At the top of the main window, click **Block Traffic**.
2. Use Symantec Client Firewall tools to address the security problem.
3. When you have fixed the problem, click **Allow Traffic**.

Customizing Symantec Client Firewall

The default Symantec Client Firewall settings should provide adequate protection for most users. If you need to make changes, use the Options menu to access Symantec Client Firewall options. The options let you control more advanced settings.

To customize Symantec Client Firewall

1. At the top of the main window, click **Options**.
2. Select the tab on which you want to change options.

About General options

General options let you control when Symantec Client Firewall runs and select visual elements that you want to display.

Table 6-1 describes the General options.

Table 6-1 General options

Group	Description
Start Symantec Client Firewall	Select whether you want to run Symantec Client Firewall manually or automatically whenever Windows starts.
Tray Icon Settings	Display a Symantec Client Firewall icon that gives you access to program settings on the Windows taskbar. You can also include links to the following Symantec Client Firewall tools: ■ Options ■ Log Viewer ■ Statistics

Table 6-1 General options

Group	Description
Logging Level	Default: Provides details about network connections, configuration and system changes, and security alerts, including Intrusion Prevention attacks and Trojan horse attacks. Web sites, private information, and ads that are blocked are also logged. Verbose: Provides details about all of the events that are logged with the default setting. Logs user agent, information about visited sites, and cookies. Private information, Java applets, ActiveX controls, ads, and Web sites that are allowed are also logged.

About Firewall options

Firewall options let you activate advanced protection features and customize the ports that your computer uses to view Web pages. Most people do not need to change these settings.

Table 6-2 describes the Firewall options.

Table 6-2 Firewall options

Group	Description
Check access settings for external modules that programs use to connect to the Internet	Check firewall rules for each component when a program uses an external software component to connect to the Internet. This ensures that Trojan horses and other malicious programs cannot attach to a safe program and evade detection.
When one program launches another, check Internet access settings for each program	Use Program Launch Monitoring to ensure that Trojan horses and other malicious programs cannot launch and manipulate safe programs without your knowledge. When Program Launch Monitoring is active, you will be alerted whenever an unrecognized program launches another program. You can then allow or block Internet access for the unrecognized program.
HTTP ports	Specify the list of ports to filter for Java and ActiveX blocking, script blocking, confidential information, cookies, and so on. If this list is empty, private information is not filtered over HTTP. If a port that carries private information is not listed here, traffic over that port is not filtered for private information. You must restart your computer for these settings to take effect.

Table 6-2 Firewall options

Group	Description
Stealth ports	Select whether Symantec Client Firewall responds to scans on unused ports as being closed. Stealthed ports do not respond to scans.

About Secure Port options

Secure Port options let you enable and disable Secure Port technology, which secures ports blocked with Trojan rules so that no applications can use the ports. You can also add additional ports to the list.

See "Using Secure Port" on page 152.

About Protocol Filtering options

Protocol Filtering options let you selectively permit or block less common IP protocols from connecting to your computer.

See "Using Protocol Filtering" on page 155.

About Settings Manager

Settings Manager lets you back up (export) and restore (import) Symantec Client Firewall settings files.

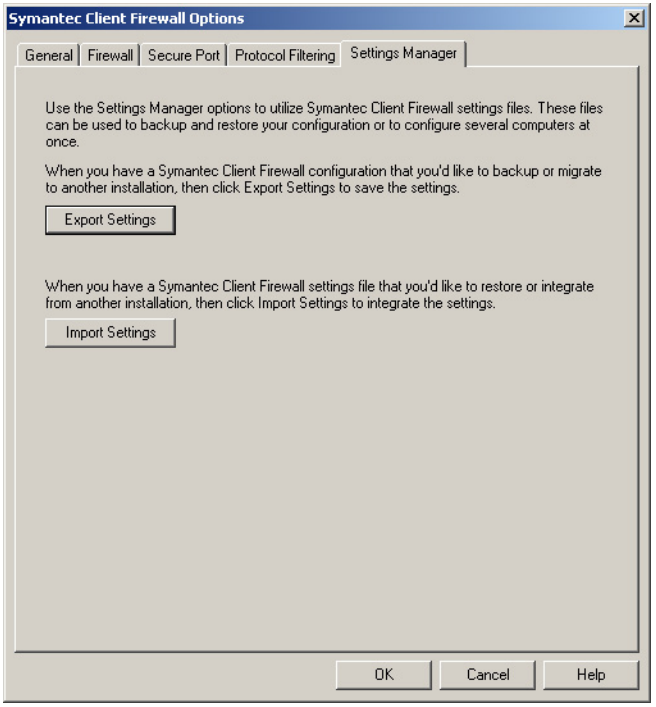
See "Exporting and importing policy files" on page 108.

Exporting and importing policy files

Symantec Client Firewall lets you export all settings, a feature that you can use to back up your firewall configuration. Symantec Client Firewall also lets you import all settings, a feature that you can use to restore your firewall configuration. You can also use the exporting and importing feature to save a known configuration to a policy file and install it on multiple computers. Exporting and importing uses XML files.

To export or import a policy file

1 At the top of the main window, click **Options**.



2 In the Symantec Client Firewall Options window, on the Settings Manager tab, select one of the following:

- Export Settings
- Import Settings

3 In the file selection dialog box, navigate to the desired directory.

4 Do one of the following:

- If you are exporting, in the File name box, type the name of the file in which to save the settings, and then click **Save**.
- If you are importing, select the target file, and then click **Open**.

5 In the Symantec Client Firewall Options window, click **OK**.

If you are exporting a policy file, do not configure settings on the other tabs before clicking OK, or the settings on the other tabs will not be exported.

Disabling Symantec Client Firewall temporarily

You might want to disable Symantec Client Firewall or one of its features temporarily in certain circumstances. For example, you might want to view online ads or see if Symantec Client Firewall is preventing a Web page from appearing correctly.

When you disable Symantec Client Firewall, the Client Firewall component, or Intrusion Prevention, you receive a protection alert that indicates that your computer is more vulnerable to security threats. You can select a preset length of time to disable Symantec Client Firewall temporarily or you can set it to enable when you restart your computer.

Note: If you disable Symantec Client Firewall and select Until system restarts as the length of time, Symantec Client Firewall is enabled only if you configured the firewall to start at system startup.

Disable Symantec Client Firewall and selected features temporarily

Disabling Symantec Client Firewall also disables all of the individual features. You can also disable individual security features. For example, you might want to see if the Client Firewall component is preventing a program from operating correctly.

To disable Symantec Client Firewall temporarily

1. In the main window, click **Status & Settings**.
2. Click **Security**.
3. On the right side of the window, click **Turn Off.**
4. In the Symantec Client Firewall Protection Alert window, select the length of time to disable Symantec Client Firewall.
5. Click **OK**.

To disable the Client Firewall component temporarily

1. In the main window, click **Status & Settings.**
2. Click **Client Firewall.**
3. On the right side of the window, click **Turn Off.**
4. In the Symantec Client Firewall Protection Alert window, select the length of time to disable the Client Firewall protection feature.
5. Click **OK.**

To disable the Intrusion Prevention feature temporarily

1. In the main window, click **Status & Settings.**
2. Click **Intrusion Prevention.**
3. On the right side of the window, click **Turn Off.**
4. In the Symantec Client Firewall Protection Alert window, select the length of time to disable the Intrusion Prevention feature.
5. Click **OK.**

To disable other protection features temporarily

1. In the main window, click **Status & Settings**.
2. Select the feature that you want to disable.
3. On the right side of the window, click **Turn Off**.

Keeping current with LiveUpdate

Symantec products depend on current information to protect your computer from newly discovered threats. Symantec makes this information available to you through LiveUpdate. Using your Internet connection, LiveUpdate obtains program updates and protection updates for your computer.

About program updates

Program updates are minor improvements to your installed product. These differ from product upgrades, which are newer versions of entire products. Program updates that have self-installers to replace existing software code are called patches. Patches are usually created to extend operating system or hardware compatibility, adjust a performance issue, or fix bugs.

LiveUpdate automates the process of obtaining and installing program updates. It locates and obtains files from an Internet site, installs them, and then deletes the leftover files from your computer.

About protection updates

Protection updates are files available from Symantec, by subscription, that keep your Symantec products up to date with the latest anti-threat technology. The protection updates that you receive depend on which product you are using.

When you should update

Run LiveUpdate as soon as you have installed your product. Once you know that your files are up to date, run LiveUpdate regularly to obtain updates. For example, to keep your virus protection current, you should use LiveUpdate once a week or whenever new viruses are discovered. Program updates are released on an as-needed basis.

About running LiveUpdate on an internal network

If you run LiveUpdate on a computer that is connected to a network that is behind a company firewall, your network administrator might set up an internal LiveUpdate server on the network. LiveUpdate should find this location automatically.

If you have trouble connecting to an internal LiveUpdate server, contact your network administrator.

Obtaining updates from the Symantec Web site

When new updates become available, Symantec posts them on the Symantec Web site. If you can't run LiveUpdate, you can obtain new updates from the Symantec Web site.

Note: Your subscription must be current to obtain new protection updates from the Symantec Web site.

To obtain updates from the Symantec Web site

1. On the Internet, go to:
   http://securityresponse.symantec.com
2. Follow the links to obtain the type of update that you need.

Obtaining updates using LiveUpdate

LiveUpdate checks for updates to all of the Symantec products that are installed on your computer.

Note: Some program updates might require you to restart your computer after you install them.

To obtain updates using LiveUpdate

1. At the top of the main window, click **LiveUpdate**.
2. In the LiveUpdate window, click **Next** to locate updates.
3. If updates are available, click **Next** to download and install them.
4. When the installation is complete, click **Finish**.

Where to get more information about Symantec Client Firewall

Symantec Client Firewall provides online Help, the Client Guide in PDF format, and links to the Symantec Response Center, Knowledge Base, and Technical Support Web sites.

Accessing Help

Help is always available throughout Symantec Client Firewall. Help buttons or links to more information provide information specific to the task that you are completing. The Help menu provides a comprehensive guide to all product features and tasks that you can complete.

To access Help

1. At the top of the main window, click **Help & Support**.
2. On the main Help menu, click **Symantec Client Firewall Help**.
3. In the Help window, in the left pane, select one of the following tabs:
   - Contents: Displays the Help by topic
   - Index: Lists Help topics in alphabetical order by keyword
   - Search: Opens a search field where you can enter a word or phrase

Accessing window and dialog box Help

Window and dialog box Help provide information about the Symantec Client Firewall program. This type of Help is context-sensitive, meaning that it provides help for the dialog box or window that you are currently using.

To access window or dialog box Help

- Click the **More Info** link if one is available.

Accessing the Client Guide PDF

The Client Guide is provided on the Symantec Client Security CD in PDF format.

Access the Client Guide PDF

You must have Adobe® Acrobat® Reader® installed on your computer to read the PDF. Once you have installed Adobe Acrobat Reader, you can read the PDF from the CD.

To install Adobe Acrobat Reader

1. Insert the Symantec Client Security CD into the CD-ROM drive.
2. Click **Browse CD**.
3. Double-click the **Acrobat** folder, and then double-click the **Win32** folder.
4. In the Win32 folder, double-click **adberdr60_envu.exe**.
5. Follow the on-screen instructions to select a folder for Adobe Acrobat Reader and complete the installation.

To read the Client Guide PDF from the CD

1. Insert the Symantec Client Security CD into the CD-ROM drive.
2. Click **Browse CD**.
3. Double-click the **Docs** folder.
4. Double-click **scsclnt.pdf**.

Accessing the Symantec Web site from the Symantec Client Firewall main window

The Symantec Web site provides extensive information about Symantec Client Firewall. There are several ways to access the Symantec Web site.

You can always access the Symantec Web site through your Internet browser at:

www.symantec.com

To access the Symantec Web site from the Symantec Client Firewall main window

1. At the top of the main window, click **Help & Support**.
2. Select one of the following:
   - Symantec Help and Support: Takes you to the Technical Support page of the Symantec Web site, from which you can search for solutions to specific problems, update your virus protection, and read the latest information about antivirus technology
   - Symantec Response Center: Takes you to the home page of the Symantec Security Response Web site, which lists the latest virus threats and security advisories

Chapter 7

Using Location Awareness and Zones

This chapter includes the following topics:

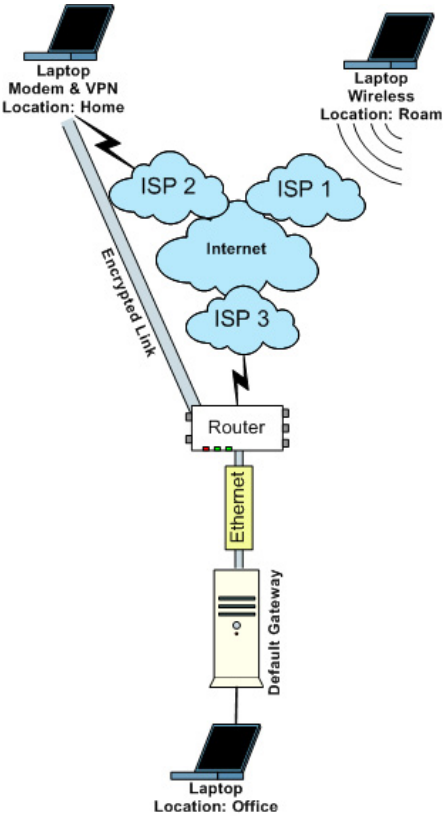
Using Location Awareness

Locations let you configure rules and Zones for different network connections made by Symantec Client Firewall. The purpose of Locations is to allow one computer to connect to different networks and automatically apply rules and Zones tailored for the different networks.

For example, you may have a specific collection of rules and Zones that you want Symantec Client Firewall to enforce when a client connects to a network using a remote wireless connection, and you may have another collection that you want Symantec Client Firewall to enforce when a client connects to a network using a local Ethernet connection.

Figure 7-1 illustrates the concept of one laptop connecting to the Internet using a wireless connection, connecting to the home office using a VPN connection across the Internet, and connecting to the office network.

Figure 7-1 One laptop connecting from different Locations



The laptop generates network traffic that differs when it connects from the three Locations, and it connects to different default gateways when it connects from the three Locations. For example, the home user VPN traffic travels over ports implemented by the VPN vendor and connects to a default gateway at ISP 2. The roaming user wireless traffic travels over other ports, uses an SSID to authenticate, and connects to a default gateway at ISP 1. The office user Ethernet traffic travels over ports used by the infrastructure operating systems, for example, Windows or Netware, and connects to an internal default gateway.

If you implement Symantec Client Firewall rules in a default deny condition, where traffic is blocked if it is not permitted with a rule, you can configure three different rulebases that permit network traffic from the three Locations. One policy file can be configured with different information for up to 64 Locations.

After installation, Symantec Client Firewall is configured with the following four Locations:

- Office
- Home
- Away
- Default

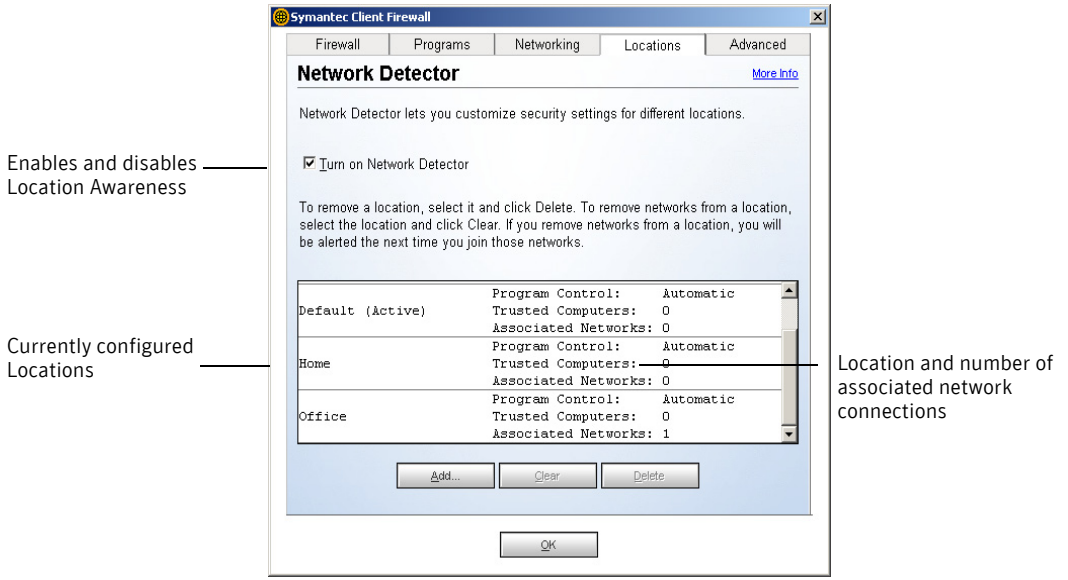
Rules can be associated with one, some, or all Locations. Zones are associated with specific Locations only. When you configure rules and Zones, you must select Locations for the rules and Zones. The Default Location is used when Location Awareness is disabled.

Enabling and disabling Location Awareness

You are not required to use Location Awareness. When Location Awareness is disabled, the rules and Zones associated with the Default Location are used. The triggering mechanism for Location Awareness is the Network Detector.

Figure 7-2 shows where you enable and disable the Network Detector.

Figure 7-2 Locations tab



The Locations tab (Network Detector window) also shows the currently configured Locations and the number of associated network connections. When the Default Location is active, the number of associated network connections is always 0, because network specifications cannot be associated with the Default Location.

To enable or disable Location Awareness

1. In the main window, click **Status & Settings**.
2. Double-click **Client Firewall**.
3. In the Symantec Client Firewall window, on the Locations tab, do one of the following:
   - To enable Location Awareness, check **Turn on Network Detector**.
   - To disable Location Awareness, uncheck **Turn on Network Detector**.

Selecting Locations to implement

When you connect to a network that is not associated with a Location, which will happen the first time that you use Symantec Client Firewall and enable Location Awareness, the firewall prompts you to select a Location to associate with the network connection information.

Table 7-1 lists the network connection information that Symantec Client Firewall may use to associate with the selected Location.

Table 7-1 Network connection information

Attribute	Description
Gateway MAC address	The Media Access Control (MAC) address of the default gateway
Gateway IP address	The IP address of the default gateway
Subnet address	The IP address and subnet mask of the client computer
Domain	The network domain name, if available
SSID	The wireless networking service set identifier (SSID)
Dialup Number	The phone number used for remote access
Dialup Entry Description	The description of the remote access point
Interface Description	The description of the interface
Interface Type	The type of network interface

Table 7-1 Network connection information

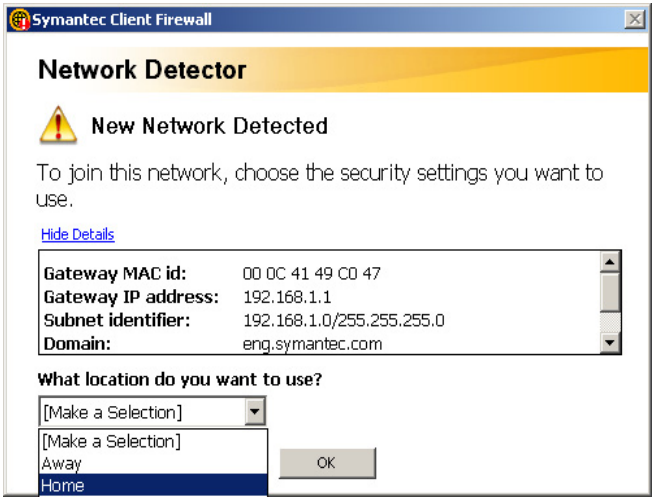
Attribute	Description
Interface Index	The index of the interface
SAV Parent Server	The Symantec AntiVirus parent management server that manages the client computer

Note: For managed Symantec Client Security clients, your firewall administrator can associate the SAV Parent Server network connection information with a Location. When Network Detector is turned on, it may not recognize the setting immediately and you may be asked to join the newly detected network by selecting a Location. Or, you may join a Location that is associated with other network connection information automatically. After communication is established with the Symantec AntiVirus parent management server, Symantec Client Firewall sets the Location that is associated with the SAV Parent Server setting as the active Location.

To select a Location to implement

1. Connect to a network with Location Awareness disabled.
   For example, display a Web page.
2. In the main window, click **Status & Settings**.
3. Double-click **Client Firewall**.
4. In the Symantec Client Firewall window, on the Locations tab, check **Turn on Network Detector**.
5. Perform some network activity.

For example, refresh a Web page.



6 In the Network Detector window, under What location do you want to use, select the Location to associate with the network connection.

7 Click **OK**.

Clearing network connection information

Each time that you associate network connection information with a Location, the Location remembers the information. It is possible to associate an excessive number of network connections with a single Location, which defeats the purpose of Location Awareness. For example, it is possible to associate information for wireless, VPN, and office connections with a single Location. Symantec Client Firewall lets you clear these associations.

To clear network connection information

1 In the main window, click **Status & Settings**.

2 Double-click **Client Firewall**.

3 In the Symantec Client Firewall window, on the Locations tab, select the Location to clear.

4 Click **Clear**.

Adding Locations

Symantec Client Firewall lets you add new Locations. You can add a new Location when the firewall detects a new connection and prompts you with the Network Detector window, and you can add a new Location from the Locations tab. In both cases, a wizard steps you through the process.

When you add a Location, all rules, Zones, and settings associated with the Default Location are automatically applied to the added Location.

To add a Location

1. In the main window, click **Status & Settings**.
2. Double-click **Client Firewall**.
3. In the Symantec Client Firewall window, on the Locations tab, click **Add**.
4. In the Setup Program Control window, select one of the following:
   - Yes: Automatically add new program rules to the Location when the firewall detects traffic that matches a known program. A prompt appears for unknown programs.
   - No: Prompt yourself to decide whether to add new program rules to the Location when the firewall detects traffic that does not match a rule.
5. Click **Next**.
6. In the Save Location window, type a Location.
7. Click **Next**.
8. In the Summary window, click **Finish**.

About customizing Location settings

When you create network Zones and firewall rules, you associate those Zones and rules with Locations.

The following tabs in the Symantec Client Firewall window let you associate Zones and rules with Locations:

- Networking
- Programs
- Advanced

Deleting Locations

Symantec Client Firewall lets you delete Locations that you added. You cannot delete any Location that was added with Symantec Client Firewall Administrator. You can add a new Location when the firewall detects a new connection and prompts you with the Network Detector window, and you can add a new Location from the Locations tab. In both cases, a wizard steps you through the process.

To delete a Location

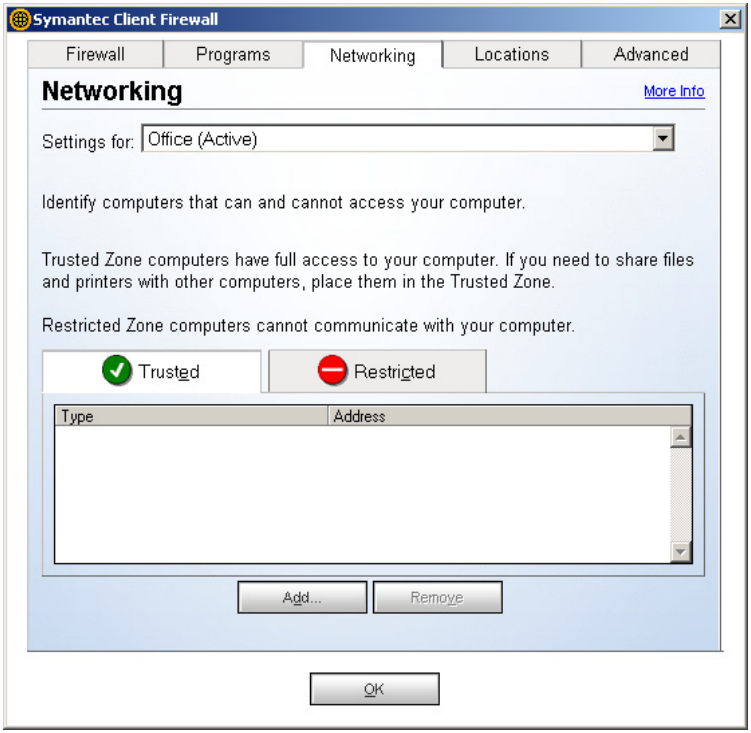
1. In the main window, click **Status & Settings**.
2. Double-click **Client Firewall**.
3. In the Symantec Client Firewall window, on the Locations tab, select the Location to delete.
4. Click **Delete**.
5. In the confirmation prompt, click **Yes**.

Adding computers to the Trusted and Restricted Zones

Symantec Client Firewall lets you organize computers on your network and computers on the Internet into two Zones that are defined by computer names or IP addresses: Trusted and Restricted. Each Zone can contain one or more entries, and each entry can specify a single computer name, a single IP address, a range of IP addresses that includes beginning and ending IP addresses, or an IP address and subnet mask.

Figure 7-3 shows the Networking tab.

Figure 7-3 Networking tab



Computers that you place in the Trusted Zone are not regulated by Symantec Client Firewall. These computers have as much access to your computer as they would have if Symantec Client Firewall was not installed. Only use the Trusted Zone for computers on your local network with which you need to share files and printers. If a computer in your Trusted Zone is attacked, and an attacker takes control of it, it poses a risk to your computer.

The firewall blocks all traffic from IP addresses listed in the Restricted Zone. The firewall does not block traffic to and from an IP address in the Restricted Zone if the address is the default gateway. The client can still access the Internet.

Additionally, Zones are attributes of Locations only. You cannot create a Zone and make it an attribute of multiple Locations. You must manually add the Zone to the other Locations. However, all Zones associated with the Default Location are automatically associated with all new Locations created with the Location wizard.

Settings for Rules, Intrusion Prevention monitoring, Web Content, Privacy Control, and Ad Blocking are ignored for Web sites with IP addresses that fall into Trusted Zones.

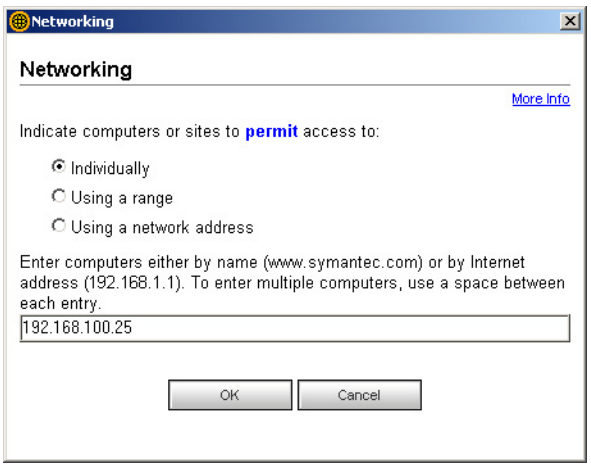
You cannot modify or delete computers that your firewall administrator adds to the Trusted and Restricted Zones. These entries appear dimmed in the user interface.

Note: Network Zones monitor common IP network traffic, which includes TCP, UDP, and ICMP protocols. Network Zones do not affect Protocol Filtering, which lets you permit or block extended IP protocols. For example, if Protocol Filtering is set to block VPN protocols that are transported over IP, these protocols are blocked for computers in the Trusted Zone. Also, if Protocol Filtering is set to permit the VPN protocols, these protocols are permitted for computers in the Restricted Zone.

See "Using Protocol Filtering" on page 155.

To add computers to the Trusted or Restricted Zone

1. In the main window, click **Status & Settings**.
2. Double-click **Client Firewall**.
3. In the Symantec Client Firewall window, on the Networking tab, in the Settings for drop-down list, select the Location for which to add a Zone.
4. On the Trusted or Restricted tab, click **Add**.



5 In the Networking dialog box, select one of the following:

- Individually: A single IP address that identifies the computer or the computer name (www.symantec.com)
- Using a range: An inclusive range of IP addresses, from the starting IP address to the ending IP address
- Using a network address: An inclusive range of IP addresses that are created by typing one IP address and a subnet mask

6 In the text box, type the IP addresses or names of the computers that you want to add to the Trusted or Restricted Zone.

7 Click **OK**.

8 On the Networking tab, click **OK**.

Chapter 8

Guarding against intrusion attempts

This chapter includes the following topics:

About guarding against intrusion attempts

Network attacks take advantage of the way that computers transfer information. Symantec Client Firewall can protect your computer by monitoring the information that comes into and out of your computer, and by blocking attack attempts.

Information travels across the Internet in the form of packets. Each packet includes a header that contains information about the sending computer, the intended recipient, how the data in the packet should be processed, and the port that should receive the packet.

Ports are channels that divide the stream of information coming from the Internet into separate paths that are handled by individual programs. When Internet programs run on a computer, they listen to one or more ports and accept information sent to these ports.

Network attacks are designed to take advantage of weaknesses in specific Internet programs. Attackers use tools that send packets containing malicious programming code to a particular port. If a program that is vulnerable to this attack is listening to that port, the code can let the attacker gain access to, disable, or even take control of the computer. The programming code that is used to generate the attacks may be contained inside of a single packet or span several packets.

How Symantec Client Firewall protects against network attacks

Symantec Client Firewall includes two tools that protect your computer from intrusion attempts, malicious Web content, and Trojan horses:

- Symantec Client Firewall: Monitors all Internet communication and creates a shield that blocks or limits attempts to view information on your computer
- Intrusion Prevention: Analyzes all incoming and outgoing information for data patterns that are typical of an attack

How Symantec Client Firewall monitors communications

When Symantec Client Firewall is active, it monitors communications between your computer and other computers on the Internet.

Table 8-1 lists common security problems that Symantec Client Firewall monitors.

Table 8-1 Common security problems

Problem	Protection
Improper connection attempts	Warns you of any connection attempts from other computers and attempts by programs on your computer to connect to other computers
Trojan horses	Notifies you when your computer encounters destructive programs that are disguised as something useful
Security and privacy incursions by malicious Web content	Monitors all Java applets and ActiveX controls and lets you select whether to run or block the program
Port scans	Cloaks inactive ports on your computer and detects port scans

Table 8-1 Common security problems

Problem	Protection
Intrusions	Detects and blocks malicious traffic and attempts by outside users to attack your computer, and scans outgoing traffic to prevent the spread of worms

You can control the level of protection by using the Security Level slider. You can also control how Symantec Client Firewall reacts to improper connection attempts, Trojan horses, and malicious Web content.

See "Customizing firewall protection" on page 133.

How Intrusion Prevention analyzes traffic

Symantec Client Firewall contains major improvements to Intrusion Prevention, including smarter attack signatures that are less likely to allow an intrusion attack, and a stateful engine that tracks all incoming and outgoing traffic. A new Intrusion Prevention engine and corresponding set of attack signatures contain these improvements, and are installed on Symantec Client Firewall by default.

Intrusion Prevention scans each packet that enters and exits your computer for attack signatures, arrangements of information that identify an attacker's attempt to exploit a known operating system or program vulnerability. In addition to blocking known variants of attacks, Intrusion Prevention now checks for possible variations of attacks and blocks them as well. For example, a hacker can modify an attack by changing the information that an attack signature uses to identify the intrusion attempt. Firewalls that rely on exact signature matches do not detect this attack. Intrusion Prevention blocks this type of intrusion attempt by anticipating as many conceivable variants in the attack signature as possible.

Table 8-2 lists examples of attacks that Symantec Client Firewall monitors.

Table 8-2 Monitored attacks

Attack	Description
BEAGLE_A_B_BACKDOOR_ACCOUNCE	A backdoor that is included with the W32.Beagle.A@mm worm. This backdoor announces its presence to the owner of the worm, which allows the attacker to issue commands, download files, and execute other malicious actions.
WINDOWS_LOCATORSVC_OVERFLOW	A method of exploiting the Microsoft Windows RPC (Remote Procedure Call) Locator service to execute malicious commands or crash the computer.

Table 8-2 Monitored attacks

Attack	Description
MS_MESSENGER_BO	An attack on the Microsoft Messenger Service that can result in a denial of service or execution of malicious code.
Bonk	An attack on the Microsoft TCP/IP stack that can crash the attacked computer.
RDS_Shell	A method of exploiting the Remote Data Services component of the Microsoft Data Access Components that lets a remote attacker run commands with system privileges.
WinNuke	An attack that can use NetBIOS to crash older Windows 95/98/NT computers.

Because attacks might span packets, Intrusion Prevention examines packets in two different ways. It scans each packet individually, looking for patterns that are typical of an attack. It also monitors the packets as a stream of information, which lets it identify attacks that are spread across multiple packets. Additionally, Intrusion Prevention remembers traffic patterns and partial patterns, and applies this information to subsequent traffic to and from your computer.

If the information matches a known attack, Intrusion Prevention automatically discards the packet and severs the connection with the computer that sent the data. This protects your computer from being affected in any way.

You can modify how Intrusion Prevention responds to attacks by excluding attack signatures from being monitored, and by enabling or disabling AutoBlock, which automatically blocks all communication to and from an attacking computer. By excluding certain network behavior from blocking, you can continue to be productive, even while your computer is under attack.

Along with protecting your computer against attacks, Symantec Client Firewall also monitors all of the information that your computer sends to other computers. This ensures that your computer cannot be used to attack other users or be exploited by zombie programs. Zombies are programs that can be secretly installed and run remotely to aid in a collective attack on another computer. If Symantec Client Firewall detects that your computer is sending information that is typical of an attack, it immediately blocks the connection and warns you about the possible problem.

To reduce the number of warnings that you receive, Symantec Client Firewall only monitors attacks that are targeted at ports that your computer uses. If an attacker attempts to connect to your computer via an inactive port or a port that has been blocked by the firewall, Symantec Client Firewall will not notify you because there is no risk of an intrusion.

Symantec Client Firewall does not scan for intrusions by computers in your Trusted Zone. However, Intrusion Prevention does monitor the information that you send to Trusted computers for signs of zombies and other remote control attacks.

Intrusion Prevention relies on an extensive list of attack signatures to detect and block suspicious network activity. Run LiveUpdate regularly to ensure that your list of attack signatures is up to date.

See "Keeping current with LiveUpdate" on page 111.

Note: If the Threat Tracer option Client firewall auto blocks IP address of the source computer is enabled in Symantec AntiVirus, Symantec Client Firewall blocks the attacking computer even if the computer is included in the Trusted Zone or the AutoBlock Exclusions list.

Customizing firewall protection

The default firewall settings should provide you with adequate protection. If the default protection is not appropriate, you can customize the firewall using the Security Level slider. The slider lets you select preset groups of security settings. You can also customize the firewall by changing individual security settings.

Changing the Security Level slider

The Security Level slider lets you select Low, Medium, or High security settings. When you change the slider position, the protection level changes. Changing the Security Level slider does not affect the protection that is provided by Intrusion Prevention.

To change the Security Level slider

1 In the main window, click **Status & Settings**.

2 Double-click **Client Firewall**.

3 In the Symantec Client Firewall window, on the Firewall tab, move the slider to the Security Level that you want. You have the following options:

High	The firewall blocks everything until you allow it. If you have run a Program Scan, you should not be interrupted frequently with Program Control alerts. You are alerted each time that an ActiveX control or Java applet is encountered. Unused ports do not respond to connection attempts, giving them a stealth appearance.
Medium (recommended)	The firewall blocks everything until you allow it. If you have run a Program Scan, you should not be interrupted frequently with Program Control alerts. ActiveX controls and Java applets run without warning. Unused ports do not respond to connection attempts, giving them a stealth appearance.

Low	The firewall permits everything that is not specifically blocked. ActiveX controls and Java applets run without warning. Unused ports do not respond to connection attempts, giving them a stealth appearance. All outgoing connections are allowed.

4 Click **OK**.

Changing individual security settings

If the default Security Level options do not meet your needs, you can change the settings for Symantec Client Firewall, Java, and ActiveX protection levels. Changing an individual setting overrides the Security Level, but it does not change the other security settings in that level.

To change individual security settings

1 In the main window, click **Status & Settings**.

2 Double-click **Client Firewall**.

3 In the Symantec Client Security window, on the Firewall tab, click **Custom Level**.

4 In the Customize Security Settings window, do one or more of the following:

- In the Client Firewall drop-down list, select a level. You have the following options:

High	Blocks all communication that you do not specifically allow. You must create firewall rules for every program that requests Internet access.
Medium	Permits all communications that are not specifically blocked.

- In the Java Applet Security or ActiveX Control Security drop-down list, select a level. You have the following options:

High	Blocks your browser from running any Java applets or ActiveX controls over the Internet. This is the safest, but most inconvenient, option. Some Web sites might not operate properly using this setting.
Medium	Prompts you when Java applets and ActiveX controls are encountered. This lets you temporarily or permanently allow or block each Java applet and ActiveX control that you encounter. It can be bothersome to respond every time that you encounter a Java applet and ActiveX control, but it lets you decide which ones to run.
None	Lets Java applets and ActiveX controls run whenever you encounter them.

- To be notified whenever unknown programs access the Internet, check **Enable Access Control Alerts**.
- To be notified whenever a remote computer attempts to connect to a port that no program is using, check **Alert when unused ports are accessed**.

5 Click **OK**.

6 On the Firewall tab, click **OK**.

Resetting security settings to defaults

Setting a custom security level disables the Security Level slider. To use the slider to select a preset security level, you must reset the security level.

To reset security settings to defaults

1. In the main window, click **Status & Settings**.
2. Double-click **Client Firewall**.
3. In the Symantec Client Security window, on the Firewall tab, click **Default Level**.
   This resets your security level to Medium. Use the Security Level slider to select one of the other preset security levels.

Customizing firewall rules

Firewall rules control how Symantec Client Firewall protects your computer from malicious incoming traffic, programs, and Trojan horses, and stops malicious outgoing traffic. The firewall automatically checks all traffic to and from your computer against these rules. Rules fall into three categories:

- General: Control protection using packet filtering, which affects all programs
- Program: Permit or block programs from accessing the Internet
- Trojan horse: Protect against malicious programs

Your firewall administrator must provide you with the appropriate permissions to customize firewall rules and to use any of the firewall features.

See "About Symantec Client Firewall permissions" on page 103.

Creating new firewall rules

Symantec Client Firewall includes Program Control, which automatically creates firewall rules for known programs as you use the Internet. You can also create and modify rules manually. All rules are associated with one or more Locations.

There are four ways to create firewall rules with Program Control:

Enable Automatic Program Control	Automatically configures access for well-known programs the first time that users run them. This option is the easiest way to set up firewall rules. You enable and disable this option for each Location.
Use Program Scan	Finds and configures access for all Internet-enabled programs on a computer at once. You can add rules to the Locations that you specify.
Respond to alerts	Warns users when known programs attempt to access the Internet for the first time if Automatic Program Control is off, and when unknown programs attempt to access the Internet. Users can then allow or block Internet access for the program. You can add rules to the current Location only.
Manually add General, Program, and Trojan rules	Lets users closely manage the list of programs and services that can access the Internet. You can add rules to one or more Locations.

Enabling Automatic Program Control

When Automatic Program Control is active, Symantec Client Firewall can automatically configure Internet access settings for programs the first time that they run. Automatic Program Control only configures Internet access for the versions of programs that Symantec has identified as safe.

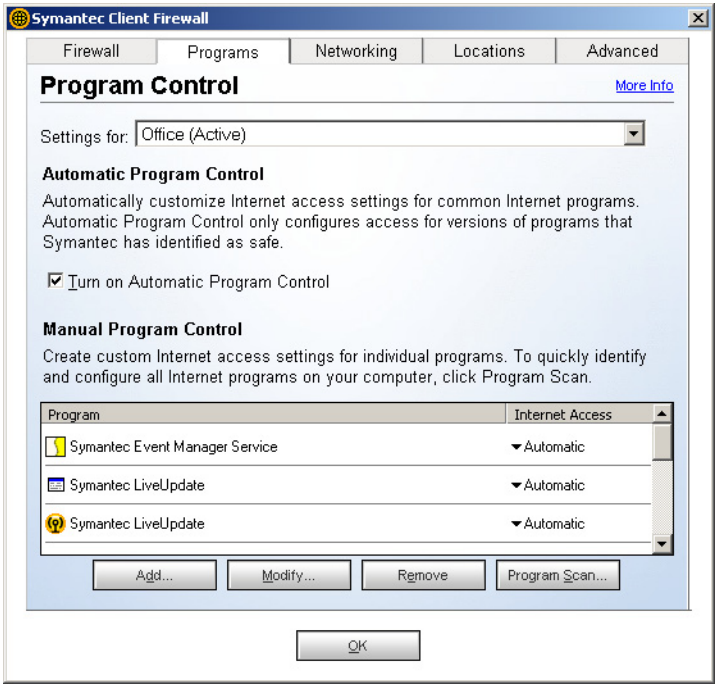
If an unknown program or an unknown version of a known program attempts to access the Internet, Symantec Client Firewall warns the user. The user can then allow or block Internet access for the program.

Note: If you create a Program rule for an application, Symantec Client Firewall might override the Program rule. This happens when Automatic Program Control determines that the rules that you created are insufficient based on the type of Internet access that the application requires.

To enable Automatic Program Control

1 In the main window, click **Status & Settings**.

2 Double-click **Client Firewall**.



3 In the Symantec Client Firewall window, on the Programs tab, in the Settings for drop-down list, select the Location for which to enable Automatic Program Control.

4 Check **Turn on Automatic Program Control**.

5 Click **OK**.

Scanning for and adding Internet-enabled programs

Scanning for Internet-enabled programs is the quickest way to set up firewall rules with Program Control. Symantec Client Firewall scans the computer for programs that it recognizes and lets you select appropriate settings for each program.

Note: Your administrator can block programs from running for certain Locations. If these programs are found when scanning your computer, rules are created for the allowed Locations only.

To scan for and add Internet-enabled programs

1. In the main window, click **Status & Settings**.
2. Double-click **Client Firewall**.
3. In the Symantec Client Firewall window, on the Programs tab, click **Program Scan**.
4. In the Program Scan window, select the disk or disks on your computer that you want to scan.
5. Click **Next**.
6. Do one of the following:
   - Check programs that you want to add to the Internet-enabled programs list.
   - Click **Check All** to add all Internet-enabled programs at once.
   - Click **Add** to manually add a program.
   - Select a program and click **Modify** to change the program settings.
7. Click **Next**.
8. Do one of the following:
   - Select the Locations to associate with the program.
   - Click **Check All** to associate the program with all Locations.
9. Click **Finish**.
10. On the Programs tab, click **OK**.

Adding a program to Program Control

You can add programs to Program Control to strictly control a program's ability to access the Internet. This overrides any settings made by Automatic Program Control.

To add a program to Program Control

1. In the main window, click **Status & Settings**.
2. Double-click **Client Firewall**.
3. In the Symantec Client Firewall window, on the Programs tab, in the Settings for drop-down list, select the Location for which to add a Program rule.
4. Click **Add**.
5. Browse to and select the program's executable file.
6. Click **Open**.
7. In the Internet Access Control alert, select the access level that you want this program to have. You have the following options:

Automatically configure Internet access (Recommended)	Use the default Symantec Client Firewall settings for this program. This option does not always appear.
Permit	Allow all access attempts by this program.
Block	Deny all access attempts by this program.
Manually configure Internet Access	Create rules controlling how this program accesses the Internet.

8. If you want to see any risks that this program could pose to your computer, click **Show Details**.
9. Click **OK**.
10. On the Programs tab, click **OK**.

Changing Program Control settings

After using Symantec Client Firewall for a while, you may find that you need to change access settings for programs. For example, you can choose to block any future Internet connections by a program or grant Internet access to a blocked program. Any changes override settings made by Automatic Program Control.

To change Program Control settings

1. In the main window, click **Status & Settings**.
2. Double-click **Client Firewall**.
3. In the Symantec Client Firewall window, on the Programs tab, in the Settings for drop-down list, select the Location that contains the Program rule to change.
4. In the list of programs, select the program that you want to change.
5. Click **Modify**.
6. In the Program Control alert, select the access level that you want this program to have. You have the following options:

Automatically configure Internet access (Recommended)	Use the default Symantec Client Firewall settings for this program. This option does not always appear.
Permit	Allow all access attempts by this program.
Block	Deny all access attempts by this program.
Manually configure Internet Access	Create rules controlling how this program accesses the Internet.

7. Click **OK**.
8. On the Programs tab, click **OK**.

About creating firewall rules manually

While Symantec Client Firewall automatically creates most of the firewall rules that you need, you may want to add specific rules. Only experienced Internet users should create their own firewall rules.

Firewall rules define specific types of communication that are either allowed or blocked. Before adding or modifying rules, be sure you understand the elements of a firewall rule.

Action options

Action options let you specify whether the rule permits, blocks, or monitors the type of network communication defined within the rule.

Table 8-3 describes the available Action options.

Table 8-3 Action options

Option	Description
Permit	Allows communication of this type to take place.
Block	Prevents communication of this type from taking place.
Monitor	Updates the Firewall tab in the Symantec Client Firewall Event Log when tracking is enabled. Rule processing then continues until a match is found. If there is no match, the communication is either blocked by default or an Internet Access Control alert appears.

Use the Monitor action sparingly. The resulting action of configuring a rule to monitor rather than permit or block depends on how a few client settings are configured. For example, if the Client Firewall level is set to High, Access Control Alerts is set to Enable, and Automatic Program Control is set to Enable, Symantec Client Firewall automatically and transparently creates a rule that permits known applications to access the Internet on the client computer. Other combinations of client settings cause the firewall to transparently block traffic that is configured with a Monitor action, or cause the firewall to prompt users to decide whether to permit or block the traffic.

Table 8-4 shows the resulting actions that the firewall takes when the Client Firewall slider level is set to High, along with possible combinations of enabled or disabled Access Control Alerts and Automatic Program Control settings.

Table 8-4 Monitor action results with Client Firewall level set to High

Access Control Alerts status	Automatic Program Control status	Resulting firewall action
Disabled	Disabled	Block.
Enabled	Disabled	Permit or block (user choice).
Disabled	Enabled	Block for unknown applications. Permit rule is automatically created for known applications.
Enabled	Enabled	Permit or block for unknown applications (user choice). Permit rule is automatically created for known applications.

Direction options

Direction options let you specify whether the rule applies to inbound network communication, outbound network communication, or network communication in both directions.

Table 8-5 describes the available Direction options.

Table 8-5 Direction options

Option	Description
Connections to other computers	The rule applies to outbound connections from your computer to another computer.
Connections from other computers	The rule applies to inbound connections from another computer to your computer.
Connections to and from other computers	The rule applies to inbound connections as well as outbound connections.

Note: Symantec Client Firewall uses stateful inspection for TCP connections. Therefore, the firewall permits inbound traffic that replies to outbound traffic. As a result, you only need to create outbound rules for client-initiated traffic, such as HTTP.

See "About stateful inspection" on page 146.

Computer options

Computer options let you specify the computers and network adapters to which a rule applies. The computers that you specify are computers with which you want to control communications.

Table 8-6 describes the available Computer options.

Table 8-6 Computer options

Option	Description
Any computer	The rule applies to all computers.
Only the computers and sites listed below	The rule applies to one computer, to multiple computers with IP addresses in a specified range, or to multiple computers in a domain.
Network Adapters	The rule applies to a specific network adapter in your computer. The IP address of the network adapter to which the rule should apply is specified.

Protocol options

Protocol options let you specify the communications protocols that a rule controls.

Table 8-7 describes the available Protocol options.

Table 8-7 Protocol options

Option	Description
TCP	The rule applies to Transmission Control Protocol (TCP) communications.
UDP	The rule applies to User Datagram Protocol (UDP) communications.
TCP and UDP	The rule applies to both TCP and UDP communications.
ICMP	The rule applies to Internet Control Message Protocol (ICMP) communications. ICMP applies to General rules and Trojan rules only.

Port options

Port options let you specify the types of communications, or ports, that are controlled by a rule.

Table 8-8 describes the available Port options.

Table 8-8 Port options

Option	Description
All types of communications (all ports)	The rule applies to communications using any port.
Only the types of communications or ports listed below	The rule applies to the ports listed. You can add ports to, and remove ports from, the list. If you specify local and remote ports, the traffic being monitored must use the local and remote ports for the rule to match.

Tracking options

Tracking options let you specify whether the program should notify you or create an Event Log entry when a network communication event matches the criteria set for this rule.

Table 8-9 describes the available Tracking options.

Table 8-9 Tracking options

Option	Description
Create an Event Log entry	An entry is created in the firewall Event Log when a network communication event matches this rule. When this feature is enabled, you can specify event frequency next to Only log event after it occurs X times.
Notify me with a Security Alert	A Security Alert dialog box appears when a network communication event matches this rule.

Description

Description lets you specify the name of the rule so that you can distinguish it from other rules.

Location options

Location options let you select the Locations with which to associate the rule.

About stateful inspection

Symantec Client Firewall uses stateful inspection, a process that creates a connection state table that tracks information about current connections such as source and destination IP addresses, ports, applications, and so forth. Symantec Client Firewall makes traffic flow decisions using this connection information before inspecting General and Program rules.

For example, if a firewall rule permits a client to connect to a Web server, the firewall logs connection information in the state table. When the server replies, the firewall checks the state table, discovers that a response from the Web server to the client is expected, and permits the Web server traffic to flow to the initiating client without inspecting the rulebase. A rule must permit the initial outbound traffic before the firewall logs the connection in the state table.

Stateful inspection allows you to simplify rulebases because you don't have to create rules that permit traffic in both directions for traffic typically initiated in one direction only. Client traffic typically initiated in one direction includes Telnet (port 23), FTP (ports 20 and 21), HTTP (port 80), and HTTPS (port 443).

Clients initiate this traffic outbound so you only have to create a rule that permits outbound traffic for these protocols. The firewall permits the return traffic when it inspects the state table.

By configuring outbound rules only, when possible, you increase client security in two ways:

- Reduce rulebase complexity.
- Eliminate the possibility that a worm or other malicious program can initiate connections to a client on ports configured for outbound traffic only. You can also configure inbound rules only, for traffic to clients that clients do not initiate.

Stateful inspection supports all rules that direct TCP traffic. Stateful inspection does not support rules that filter UDP and ICMP traffic. For UDP and ICMP, you must create rules that permit traffic in both directions when necessary. For example, if you want clients to use the ping command and receive replies, you must create a rule that permits ICMP traffic in both directions.

Priorities for firewall rule processing

When a computer attempts to connect to your computer, or when your computer attempts to connect to a computer on the Internet, Symantec Client Firewall compares the type of connection with its list of firewall rules.

Firewall rules are processed in a set order beginning with the state table. For example, if inbound traffic is responding to outbound traffic, the firewall first inspects the state table, discovers that the inbound traffic is expected, and permits the traffic. Even if a rule exists to block inbound return traffic, the blocking rule is never processed.

After the state table, rule processing is based on whether rules are locked or unlocked. All rules created with Symantec Client Firewall are unlocked. Rules created with Symantec Client Firewall Administrator and exported to Symantec Client Firewall can be locked or unlocked.

Table 8-10 lists the order in which Symantec Client Firewall processes firewall rules.

Table 8-10 Rule processing priority

Priority	Rule type	User type
First	General	Locked
Second	Program	Locked
Third	General	Unlocked

Table 8-10 Rule processing priority

Priority	Rule type	User type
Fourth	Program	Unlocked
Fifth	Trojan	Locked
Sixth	Trojan	Unlocked

Note: The Secure Port utility secures ports defined with Trojan rules so completely that all Trojan rules configured as Block take first priority for outbound traffic only.

See "Using Secure Port" on page 152.

Adding firewall rules

Before adding a new firewall rule, you must first determine whether you want to add a firewall rule that controls general access to the Internet or a firewall rule that controls a program.

The following types of rules are available:

- General rules affect all applications accessing the Internet because they inspect all packets.
- Program rules control one program's access to the Internet. Use Program rules when you have a program that needs access to the Internet.
- Trojan rules are typically used to block ports used by Trojan horses. These rules also inspect all packets but are inspected after General and Program rules.

Adding General rules

You can create General firewall rules that apply to all of the programs on your computer.

To add a General rule

1. In the main window, click **Status & Settings**.
2. Double-click **Client Firewall**.
3. In the Symantec Client Firewall window, on the Advanced tab, click **General**.
4. In the General Rules window, click **Add**.

5 Follow the on-screen instructions.

6 On the Advanced tab, click **OK**.

Adding Program rules

You can create Program firewall rules that apply to specific programs on your computer.

To add a Program rule

1 In the main window, click **Status & Settings**.

2 Double-click **Client Firewall**.

3 In the Symantec Client Firewall window, on the Programs tab, click **Add**.

4 In the Select a program dialog box, select an executable file, and then click **Open**.

5 In the Program Control alert, in the What do you want to do drop-down list, click **Manually configure Internet access**.

6 Click **OK**.

7 Follow the on-screen instructions.

8 On the Programs tab, click **OK**.

Adding Trojan rules

You can create Trojan firewall rules that apply to Trojan horse threats and co-locate them so they are inspected last. When Trojan rules configured to block traffic are matched, the IP address that initiated the traffic is automatically blocked.

See "Enabling or disabling AutoBlock" on page 161.

To add a Trojan rule

1 In the main window, click **Status & Settings**.

2 Double-click **Client Firewall**.

3 On the Advanced tab, click **Trojan Horse**.

4 In the Trojan Horse Rules dialog box, click **Add**.

5 Follow the on-screen instructions.

6 On the Advanced tab, click **OK**.

Changing existing firewall rules

You can change firewall rules if they are not functioning the way that you want. If you change a rule, the rule is changed for all Locations that implement the rule.

Note: If your administrator updates your firewall policy to block programs from running for certain Locations, you cannot modify existing Program rules that the new policy affects. You can, however, delete these Program rules. After you delete the Program rule, when the program runs again, Program rules are created only for Locations that the new policy does not restrict.

To change an existing firewall rule

1. In the main window, click **Status & Settings**.
2. Double-click **Client Firewall**.
3. Do one of the following:
   - In the Symantec Client Firewall window, on the Programs tab, in the Settings for drop-down list, select a Location that contains the rule to change.
   - In the Symantec Client Firewall window, on the Advanced tab, select General or Trojan Horse.
4. Select the rule to change.
5. Click **Modify**.
6. Follow the on-screen instructions to change any aspect of the rule.
7. When you have finished changing rules, click **OK**.

Changing the order of firewall rules

Symantec Client Firewall processes each list of firewall rules from the top down. You can determine how Symantec Client Firewall processes firewall rules by changing their order. When you change the ordering, it affects ordering for the currently selected Location only.

Note: Firewall rules can include both locked and unlocked rules. Your system administrator can lock rules, preventing you from changing their order. Locked rules always have higher priority than unlocked rules in the same rule set. You can change the order of unlocked rules only.

To change the order of a firewall rule

1. In the main window, click **Status & Settings**.
2. Double-click **Client Firewall**.
3. Do one of the following:
   - In the Symantec Client Firewall window, on the Programs tab, in the Settings for drop-down list, select the Location that contains the rules to reorder.
   - In the Symantec Client Firewall window, on the Advanced tab, select General or Trojan Horse.
4. Select the rule that you want to move.
5. Do one of the following:
   - To have Symantec Client Firewall process this rule before the rule above it, click **Move Up**.
   - To have Symantec Client Firewall process this rule after the rule below it, click **Move Down**.
6. When you are done moving rules, click **OK**.

Disabling firewall rules temporarily

You can disable a firewall rule temporarily if you need to allow specific access to a computer or program. If you disable a rule, the rule is disabled for all Locations that implement the rule.

Remember to reenable the rule when you are done working with the program or computer that required the change.

To disable a firewall rule temporarily

1. In the main window, click **Status & Settings**.
2. Double-click **Client Firewall**.
3. Do one of the following:
   - In the Symantec Client Firewall window, on the Programs tab, click **Modify**, and then uncheck the box next to the rule that you want to disable.
   - In the Symantec Client Firewall window, on the Advanced tab, select General or Trojan Horse, and then uncheck the box next to the rule that you want to disable.

Removing firewall rules

You can remove firewall rules when they are no longer necessary. When you delete a rule, the system prompts you to decide whether to delete the rule from the current or all Locations. You cannot delete General or Trojan rules that are locked, and you cannot delete Program rules that contain one or more locked rules.

To remove a firewall rule

1. In the main window, click **Status & Settings**.
2. Double-click **Client Firewall**.
3. Do one of the following:
   - In the Symantec Client Firewall window, on the Programs tab, in the Settings for drop-down list, select the Location that contains the rules to remove.
   - In the Symantec Client Firewall window, on the Advanced tab, select General or Trojan Horse.
4. Select the rule that you want to remove.
5. Click **Remove**.
6. When you are done removing rules, click **OK**.

Using Secure Port

Secure Port blocks TCP and UDP traffic on local ports defined in Trojan rules as Block and ports defined by users running Symantec Client Firewall. Secure Port secures the ports so completely that outbound traffic originating from these ports never triggers firewall rulebase inspection. Because the rulebase is not inspected for these ports, firewall alert messages never appear for these ports even when the Always Display Security Alerts feature is enabled. The rulebase is inspected for inbound traffic destined for these ports.

Additionally, when Secure Port is enabled, Windows applications that use random ports know that the ports are secured and skip them during random port sequencing. As a result, Secure Port protects clients against Trojan horses that use ports inside General permitted port ranges without interrupting networking communications.

Note: Secure Port secures ports defined as Local Block in Trojan rules only, and also secures these ports in Trusted Zones. Secure Port cannot secure ports that are in use by other programs. In addition, a Program rule must exist that blocks all inbound TCP and UDP traffic to SymSPort.exe, or Trojan horse alerts will still appear. This rule is installed by default.

Enabling and disabling Secure Port

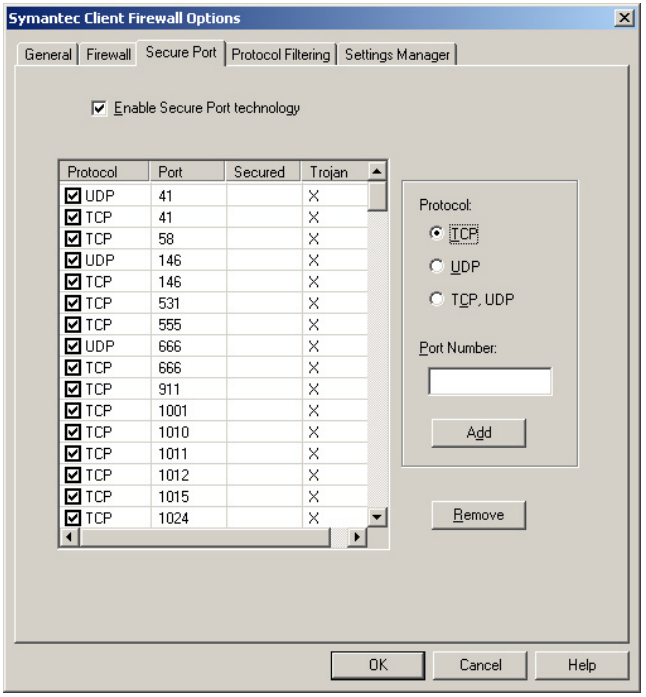
Secure Port secures all local ports defined in Trojan rules.

Enable and disable Secure Port

Secure Port lets you selectively enable and disable specific ports.

To enable Secure Port

1 At the top of the main window, click **Options**.



2 In the Symantec Client Firewall Options window, on the Secure Port tab, check **Enable Secure Port technology**, and then click **OK**.
When the ports are secured, Xs appear in the Secured column, which may take up to 30 seconds.

3 To verify that the ports are secured, reopen the Symantec Client Firewall Options window.

To disable Secure Port for individual ports

1 In the port list, in the Protocol column, uncheck the box in the row that lists the target port.

2 Click **OK**.
When the port is released, no X appears in the Secured column.

3 To verify that the port is released, reopen the Symantec Client Firewall Options window.

To enable Secure Port for individual ports

1 In the port list, in the Protocol column, check the box in the row that lists the target port.

2 Click **OK**.
When the port is secured, an X appears in the Secured column.

3 To verify that the port is secured, reopen the Symantec Client Firewall Options window.

To disable Secure Port

1 At the top of the main window, click **Options**.

2 In the Symantec Client Firewall Options window, on the Secure Port tab, uncheck **Enable Secure Port technology**, and then click **OK**.
When the ports are released, Xs disappear from the Secured column.

3 To verify that the ports are released, reopen the Symantec Client Firewall Options window.

Adding and removing user-defined ports

Secure Port lets you add and remove additional ports.

Add and remove user-defined ports

If you attempt to remove a port defined with a Trojan rule, the port becomes disabled only. The port does not disappear from the list.

To add a user-defined port to Secure Port

1. At the top of the main window, click **Options**.
2. In the Symantec Client Firewall window, on the Secure Port tab, under Protocol, select one of the following:
   - TCP
   - UDP
   - TCP, UDP
3. Under Port Number, type the port number to add.
4. Click **Add**.
   A row for the port number appears in the port list.
5. Click **OK**.

To remove a user-defined port from Secure Port

1. In the port list, right-click the row that contains the target port, and then click **Remove**.
   The row that listed the port number disappears from the port list.
2. Click **OK**.

Using Protocol Filtering

Protocol Filtering lets you permit or block incoming and outgoing traffic that uses less common IP protocols. Most network traffic uses the more common TCP, UDP, and ICMP protocols, which you configure every time that you create rules and pRules. Because many products, including VPN solutions, use less common IP protocols to communicate, you should permit all IP protocols until you are ready to research the software and devices that your network uses.

The complete IP protocol list is updated at:
www.iana.org/assignments/protocol-numbers

About VPN protocols

Virtual Private Networks (VPN) use additional protocols based on the type of communication that is needed and what type of security is used to secure the communication tunnels. The protocols that VPNs use vary. If your VPN client cannot communicate with your internal network, then the firewall might be blocking IP protocols that are necessary for the communication. For tighter security, you can permit the individual IP protocols that your VPN solution requires. You can also permit all VPN-related IP protocols if you are uncertain of which are needed in your network.

Table 8-11 lists and describes common VPN protocols.

Table 8-11 VPN protocols and their descriptions

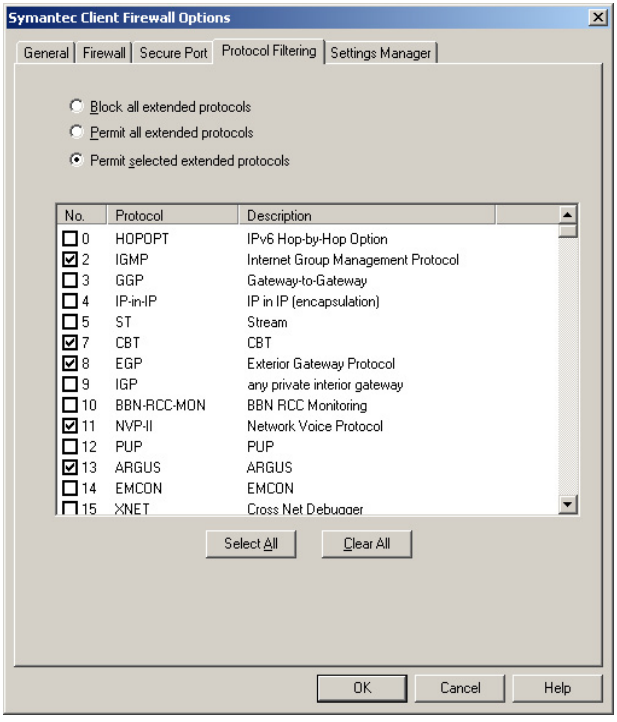
IP protocol	Description
47 - GRE	The Generic Routing Encapsulation protocol is used with VPNs that use the Microsoft Point-to-Point Tunneling Protocol (PPTP).
50 - ESP	The Encapsulation Security Payload protocol is used with VPNs that use the IPSec protocol.
51 - AH	The Authentication Header protocol is used with VPNs that use the IPSec protocol.
56 - TLSP	The Transport Layer Security Protocol uses Kryptonet key management to provide privacy and data integrity between two applications communicating over the Internet.
57 - SKIP	The Simple Key-Management for Internet Protocol is used with VPNs that use Secure Socket Layers (SSL) or IPSec protocols.
115 - L2TP	The Level 2 Tunneling Protocol is used with VPNs that use the IPSec protocol and is also Microsoft's main authentication and encryption protocol.

Permitting and blocking extended protocols

Protocol Filtering lets you permit or block all IP protocols that are not monitored through General, Program, and Trojan horse rules.

To permit and block extended protocols

1 At the top of the main window, click **Options**



2 In the Symantec Client Firewall Options window, on the Protocol Filtering tab, select the protocols that you want to permit or block.

3 Click **OK.**

Customizing Intrusion Prevention

The default Intrusion Prevention settings should provide you with adequate protection. If the default protection is not appropriate, you can customize Intrusion Prevention settings. You can customize Intrusion Prevention by excluding specific network activity from monitoring or alerting, and enabling or disabling AutoBlock.

Note: Typically, customizing Intrusion Prevention makes it less secure. You cannot exclude signatures or IP addresses if your system administrator has locked these settings.

Displaying Intrusion Prevention alerts

Symantec Client Firewall lets you specify whether to display alerts when Intrusion Prevention blocks connections.

To display Intrusion Prevention alerts

1. In the main window, click **Status & Settings**.
2. Double-click **Intrusion Prevention**.
3. On the Intrusion Prevention tab, check **Notify me when Intrusion Prevention blocks connections**.

Excluding Intrusion Prevention alerts

Symantec Client Firewall lets you exclude alerts for individual attack signatures. If you receive repeated warnings about possible attacks, and you are unsure of whether these attacks are safe or harmful, you can remain protected from these potential attacks while you continue to work without the warnings constantly appearing.

Note: For Intrusion Prevention alerts to appear, Display alerts when Intrusion Prevention blocks connections must be checked. You can then exclude individual attack signatures from generating alerts. If this setting is unchecked, potential attacks do not trigger alerts.

To exclude Intrusion Prevention alerts

1. In the main window, click **Status & Settings.**
2. Double-click **Intrusion Prevention.**

3 On the Intrusion Prevention tab, click **Advanced.**

4 In the Intrusion Prevention Signature Exclusions dialog box, in the Intrusion Prevention Signature Names list, select the attack signature that you want to exclude from alerting.

5 Click **Properties.**

6 Uncheck **Alert me when this signature is detected.**

7 Click **OK.**

Excluding network activity from being monitored

In some cases, benign network activity may appear similar to a Symantec Client Firewall attack signature. If you receive repeated warnings about possible attacks, and you know that these attacks are being triggered by safe behavior, you can create an exclusion for the attack signature that matches the benign activity.

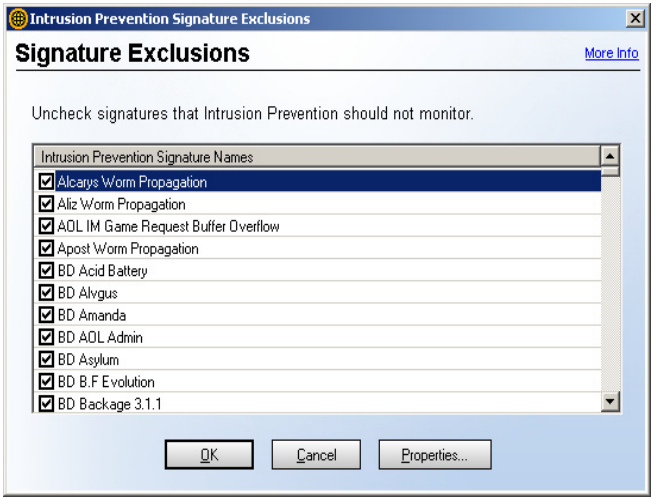
Note: Each exclusion that you create leaves your computer vulnerable to attacks and affects all IP addresses. Be very selective when excluding attacks. Only exclude behavior that is always benign. You may not be able to exclude signatures if your system administrator locked them.

To exclude attack signatures from being monitored

1 In the main window, click **Status & Settings**.

2 Double-click **Intrusion Prevention**.

3 On the Intrusion Prevention tab, click **Advanced**.



4 In the Intrusion Prevention Signature Exclusions dialog box, in the Intrusion Prevention Signature Names list, locate the attack signature that you want to exclude.

5 Uncheck the signature name.

6 When you are finished excluding signatures, click **OK**.

7 Click **OK**.

Including attack signatures

If you have excluded attack signatures that you want to monitor again, you can include them in the list of active signatures.

To include attack signatures

1 In the main window, click **Status & Settings**.

2 Double-click **Intrusion Prevention**.

3 On the Intrusion Prevention tab, click **Advanced**.

4 In the Intrusion Prevention Signature Exclusions dialog box, in the Intrusion Prevention Signature Names list, locate the attack signature that you want to monitor.

5 Select the signature name.

6 When you are done including signatures, click **OK**.

7 Click **OK**.

Enabling or disabling AutoBlock

When Symantec Client Firewall detects an attack, it automatically blocks traffic from the attacking computer to ensure that your computer is safe. Attacks include traffic specified with Trojan rules. Symantec Client Firewall can also activate AutoBlock, which automatically blocks all incoming traffic from the attacking computer and all outgoing traffic to the attacking computer for a set period of time, regardless of whether the traffic matches an attack signature.

By default, AutoBlock stops all traffic to and from the attacking computer for 30 minutes, and places the IP address of the attacking computer in the AutoBlock list.

If AutoBlock is disabled and Intrusion Prevention determines that incoming traffic matches an attack signature, your computer may receive multiple alerts for an extended period. You might consider excluding the alerts for the matched attack signature.

See "Excluding Intrusion Prevention alerts" on page 158.

Note: In the main window, Client Firewall must be enabled to process AutoBlock IP addresses. If Client Firewall is disabled, AutoBlock is disabled. Furthermore, IP addresses in trusted Zones are never added to the AutoBlock list, and AutoBlock IP addresses are associated with all Locations.

To enable or disable AutoBlock

1. In the main window, click **Status & Settings**.
2. Double-click **Intrusion Prevention**.
3. On the AutoBlock tab, do one of the following:
   - Check **Turn on AutoBlock**.
   - Uncheck **Turn on AutoBlock**.

Populating AutoBlock from Symantec Client Firewall

When Symantec Client Firewall detects an attack, it can also populate the IP address of the attacking computer in the AutoBlock list.

To populate AutoBlock from Symantec Client Firewall

1. In the Symantec AntiVirus window, click **Configure** > **File System Auto-Protect**.
2. In the File System Auto-Protect window, check **Enable Auto-Protect**.
3. Click **Advanced**.

4 In the Auto-Protect Advanced Options window, under Threat Tracer, do the following:
   - Check **Enable Threat Tracer**.
   - Check **Resolve source computer IP address**.
   - Check **Client firewall auto blocks IP address of the source computer**.
5 Click **OK**.
6 In the File System Auto-Protect window, click **OK**.

Unblocking computers that are currently blocked by AutoBlock

In some cases, Symantec Client Firewall may recognize normal activity as an attack. If you can't communicate with computers that you should be able to communicate with, they may be on the list of computers currently blocked by AutoBlock.

If a computer that you need to access appears on the list of computers currently blocked by AutoBlock, unblock it. If you have changed your protection settings and want to reset your AutoBlock list, you can unblock all of the computers on the AutoBlock list at once.

To unblock computers currently blocked by AutoBlock

1 In the main window, click **Status & Settings**.
2 Double-click **Intrusion Prevention**.
3 On the AutoBlock tab, do one of the following:
   - To unblock one computer, select its IP address, and then click **Unblock**.
   - To unblock all computers on the AutoBlock list, click **Unblock All**.

Excluding computers from AutoBlock

Some normal Internet activities are repeatedly recognized by Symantec Client Firewall as attacks. For example, some Internet service providers scan the ports of your computer to ensure that you are within their service agreements. To prevent normal activities from interrupting your Internet use, you can exclude these activities from being blocked by AutoBlock.

Note: You cannot remove computers that your system administrator has locked.

To exclude computers from AutoBlock

1. In the main window, click **Status & Settings**.
2. Double-click **Intrusion Prevention**.
3. On the AutoBlock tab, click **Exclusions**.
4. Do one of the following:
   - In the Currently blocked list, select a blocked computer, and then click **Remove**.
   - Click **Add**, and then type the computer name, IP address, IP address range, or network address that contains the computer that you want to exclude.
5. When you are done excluding computers, click **OK**.

Restricting a blocked computer

You can add a blocked computer to your Restricted Zone to permanently prevent that computer from accessing your computer. Computers added to the Restricted Zone do not appear on the blocked list because Symantec Client Firewall automatically rejects any connection attempts by restricted computers.

To restrict a blocked computer

1. In the main window, click **Status & Settings**.
2. Double-click **Intrusion Prevention**.
3. On the AutoBlock tab, in the list of computers that are currently blocked by AutoBlock, select the address to add to the Restricted Zone.
4. Click **Restrict**.
5. When you are done restricting computers, click **OK**.

Chapter 9

Securing Web browsing sessions

This chapter includes the following topics:

About protecting your privacy

Every time that you browse the Internet, computers and Web sites collect information about you. Some of this information comes from forms that you fill out and choices that you make on pages. Other information comes from your browser, which automatically provides information about the Web page that you last visited and the type of computer that you're using.

Many Web sites store information they collect in cookies that are placed on your hard disk. When you return to a site that has set a cookie on your computer, the Web server opens and reads the cookie.

Most cookies are harmless. Sites use them to personalize Web pages, remember choices that you have made on the site, and deliver optimized pages for your computer. However, sites can also use cookies to track your Internet usage and browsing habits.

Malicious users can also collect personal information without your knowledge. Any time that you send information over the Internet, the data must pass through a number of computers before it reaches its destination. During transmission, it is possible for third parties to intercept and steal this information.

Computers include some basic security features, but they might not be enough to protect your personal information. Privacy Control helps protect your privacy by giving you several levels of control over cookies and other information that your browser sends to Web sites.

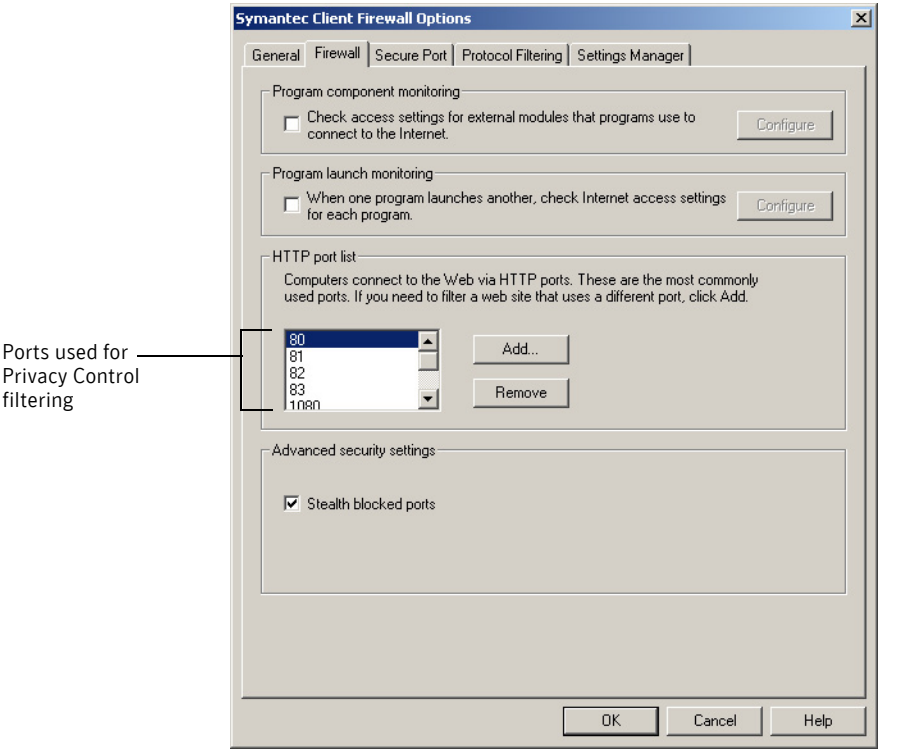
Privacy Control can also ensure that you don't send private information, such as credit card numbers, over the Internet unless they are encrypted, or you specifically allow it. Privacy Control filters plain text only.

About selecting ports to monitor for privacy

The Symantec Client Firewall Options window contains a list of ports that Privacy Control monitors.

Figure 9-1 shows the location of the port list.

Figure 9-1 HTTP port list used for Privacy Control filtering



When you select Privacy Control features and options, the assumption is that these features and options operate on these ports. If this port list is empty and Privacy Control is enabled, Privacy Control is effectively disabled because it does not know which ports to monitor.

The default ports are the most commonly used ports for Web traffic. If you use custom Web-based applications that use different ports, you must add those ports to this list if you want to implement Privacy Control on these ports.

Note: This port list applies to Privacy Control for instant messenger programs and email clients.

Identifying private information to protect

Many Web sites ask for your name, email address, and other personal information. While it is generally safe to provide this information to large, reputable sites, malicious sites can use this information to invade your privacy. It is also possible for people to intercept information sent through the Web, email messages, and instant messenger programs.

Privacy Control lets you create a list of information that you want to remain private. If you attempt to send protected information over the Internet, Symantec Client Firewall can warn you about the security risk or block the connection.

Tips on entering private information

Because Symantec Client Firewall blocks personal information exactly the way that you enter it into the program, it is better to enter only partial numbers. For example, a phone number could be typed as 888-555-1234, but it could also be typed without dashes (8885551234) or with spaces (888 555 1234), or even in two or more separate fields. One common aspect of these formats is that the last four digits (1234) are always together. Therefore, you can have better protection by protecting the last four digits than you have by protecting the entire number.

Entering partial information has two advantages. First, you are not entering a complete number where someone might find it. Second, it lets Symantec Client Firewall block your private information on sites that use multiple text boxes for phone or credit card numbers.

About Privacy Control and SSL

Most Web sites that conduct credit card transactions use Secure Sockets Layer (SSL) connections to encrypt connections between your computer and the

server. Privacy Control cannot block private information sent over SSL connections because the traffic is encrypted. However, because the information is encrypted, only the recipient of the email will be able to read the message. If necessary, you can disable the ability of your computer to establish SSL connections.

See "Customizing Privacy Control settings" on page 170.

Setting the Privacy Level

Symantec Client Firewall offers preset security levels that help you set several Privacy Control options at one time. The Privacy Level slider lets you select Low, Medium, or High protection.

To set the Privacy Level

1. In the main window, click **Status & Settings**.
2. Double-click **Privacy Control**.
3. In the Privacy Control window, move the slider to the Privacy Level that you want. You have the following options:

High	All personal information is blocked and an alert appears each time that a cookie is encountered.
Medium (recommended)	An alert appears if private information is typed into a Web form, email message, or instant messenger program. Conceals your browsed URLs from Web sites. Cookies are not blocked.
Low	Confidential information is not blocked. Cookies are not blocked. Conceals your browsing from Web sites.

4. Click **OK**.

Adding private information

You must add information that you want to protect to the Symantec Client Firewall Private Information list. If there are any Web sites that you want to allow this information to reach, you can exclude these Web sites from being monitored.

To add private information

1. In the main window, click **Status & Settings**.
2. Double-click **Privacy Control**.
3. In the Privacy Control window, click **Private Information**.

4 In the Private Information dialog box, click **Add**.

5 In the Add Private Information dialog box, in the Information category drop-down list, select a category.

6 In the Description text box, type a description to help you remember why you are protecting this information.

7 In the Information to protect text box, type the information that you want to block from being sent over nonsecure Internet connections.

8 Under Protect this private information when using, select one or more of the following programs to check for private information:

- Web
- Instant messaging
- E-Mail

Private information that passes through Web-based (HTTP) email is not protected by selecting the E-Mail setting, which monitors email programs that use Simple Mail Transfer Protocol (SMTP). Some instant messaging programs allow you to configure how to communicate with their servers. If you want to communicate by using HTTP requests, selecting the Instant messaging setting, which monitors SOCKS traffic, does not protect your instant messaging conversations. To protect your private information that passes through Web-based email and instant messaging programs, select the Web setting.

9 In the Exceptions text box, type the Web sites, if any, that you want to exclude from being protected.

10 Click **OK**.

Modifying or removing private information

You can modify or remove private information at any time.

To modify or remove private information

1 In the main window, click **Status & Settings**.

2 Double-click **Privacy Control**.

3 In the Privacy Control window, click **Private Information**.

4 In the Private Information dialog box, select the private information that you want to modify or remove.

5 Select one of the following:
- Modify
- Remove

6 Click **OK**.

Customizing Privacy Control settings

You can change the settings for Private Information, Cookie Blocking, Browser Privacy, and Secure Connections if the Privacy Level settings do not meet your needs. For example, you can block all attempts to send private information while allowing Web sites to customize their pages using your browser information.

Table 9-1 lists the areas that Privacy Control protects.

Table 9-1 Privacy Control protection areas

Protection	Description
Private Information	Blocks specific strings of text that you do not want sent over the Internet
Cookie Blocking	Stops Web sites from retrieving personal information stored in cookie files and from writing them to your hard disk
Browser Privacy	Protects information about your browsing habits and browser software
Secure Connections	Allows you to establish secure connections using SSL to online stores and other Web sites

When you customize settings, the Privacy Level sliders become unavailable.

To activate the Privacy Level sliders

1 In the main window, click **Status & Settings**.

2 Double-click **Privacy Control**.

3 In the Privacy Control window, click **Default Level**.

Changing the Private Information setting

You can change the Private Information setting to control how Symantec Client Firewall handles attempts to send information on the Private Information list over the Internet.

To change the Private Information setting

1. In the main window, click **Status & Settings**.
2. Double-click **Privacy Control**.
3. In the Privacy Control window, click **Custom Level**.
4. In the Customize Privacy Settings dialog box, select the Private Information setting that you want. You have the following options:

High	Blocks all outgoing private information
Medium	Alerts you each time that you attempt to send private information to a nonsecure Web site, or through an instant messenger program, or email message
None	Does not block private information

5. Click **OK**.

Changing the Cookie Blocking setting

Many Web sites store information that they collect in cookies placed on your hard disk. When you return to a site that has set a cookie on your computer, the Web server opens and reads the cookie. Change the Cookie Blocking setting to control how Symantec Client Firewall handles sites that attempt to place cookies on your computer.

Note: Two types of cookies exist, persistent (temporary) and non-persistent (permanent until you delete them). Symantec Client Firewall treats both types the same way.

To change the Cookie Blocking setting

1. In the main window, click **Status & Settings**.
2. Double-click **Privacy Control**.
3. In the Privacy Control window, click **Custom Level**.

4 In the Customize Privacy Settings dialog box, select the Cookie Blocking setting that you want. You have the following options:

High	Blocks all cookies
Medium	Alerts you each time that a cookie is encountered
None	Allows cookies

5 Click **OK**.

Enabling and disabling Browser Privacy

Browser Privacy is a Privacy Control feature that prevents Web sites from gathering information about your browser software and browsing habits.

Browser Privacy prevents Web sites from learning the type of browser that you are using, the Web site that you last visited, and other information about your browsing habits. Some Web sites that depend on JavaScript may not work correctly if they cannot identify the type of browser that you are using.

To enable or disable Browser Privacy

1 In the main window, click **Status & Settings**.

2 Double-click **Privacy Control**.

3 In the Privacy Control window, click **Custom Level**.

4 In the Customize Privacy Settings dialog box, do one of the following:

- To enable Browser Privacy, check **Enable Browser Privacy**.
- To disable Browser Privacy, uncheck **Enable Browser Privacy**.

5 Click **OK**.

Disabling and enabling secure Web connections

When you visit a secure Web site, your browser sets up an encrypted connection with the Web site. Private information cannot be filtered over encrypted connections. If you want to ensure that you are not sending private information to secure Web sites, you can disable secure Web connections.

If you disable secure Web connections, your browser will not encrypt any information that it sends. You should only disable secure Web connections if you are using the Private Information filter.

To enable or disable secure Web connections

1. In the main window, click **Status & Settings**.
2. Double-click **Privacy Control**.
3. In the Privacy Control window, click **Custom Level**.
4. In the Customize Privacy Settings dialog box, do one of the following:
   - To enable secure Web connections, check **Enable Secure Connections (https)**.
   - To disable secure Web connections, uncheck **Enable Secure Connections (https)**.
5. Click **OK**.

Blocking ads

Many Web sites use aggressive techniques to draw attention to the ads on their pages. Some have begun using larger, more prominent ads, while others rely on ad windows that appear when you enter or leave the site. Along with increasing the amount of time that it takes to display Web pages, some ads contain offensive content, cause software conflicts, or use tricks to open additional browser windows.

Ad Blocking helps avoid these problems. When Ad Blocking is active, Symantec Client Firewall transparently removes the following:

- Ad banners
- Pop-up and pop-under ads
- Macromedia Flash-based ads and animations

How Ad Blocking works

Symantec Client Firewall detects and blocks ads based on three criteria: their dimensions, locations, and strings.

See "About creating text strings that identify ads to block or permit" on page 180.

Blocking by dimensions

Most online advertisers use one or more standard sizes for their ads. Symantec Client Firewall now includes the ability to block images, Flash animations, and other HTML elements that have the same dimensions as these common ad sizes.

Blocking by location

Every file on the Internet has a unique address or URL. When you view a Web page, your computer connects to a URL and displays the file that is stored there. If the page points to graphics and other multimedia content, your browser displays the files as part of the page.

When you go to a Web page that includes a banner ad, the instructions used to display the page might include the following:

<p>Greetings from the Cleaning company<img src="http://www.spammersRus.com/nifty_images/image7.gif">

Your browser displays the text Greetings from the Cleaning company on the screen. Then it connects to www.spammersRus.com and requests a file called /nifty_images/image7.gif. (The suffix .gif indicates that this is a Graphics Interchange Format file, a common image file format.) The computer at www.spammersRus.com sends the file to the browser, which displays the image.

When Ad Blocking is enabled and you connect to a Web site, Symantec Client Firewall scans Web pages and compares their contents to two lists:

- A default list of ads that Symantec Client Firewall blocks automatically for all Web pages. Also, you can append the list with ads that should be blocked automatically. Ads can only be blocked for the default list.
- A list of Web sites that you create that requires specific handling for Ad Blocking. You can add to and change this list. Ads can be permitted or blocked for individual Web sites.

If the page includes files from a blocked domain, Symantec Client Firewall removes the link and downloads the rest of the page. You can also configure Ad Blocking settings for individual Web sites.

See “Configuring Ad Blocking settings” on page 180.

Enabling and disabling Ad Blocking

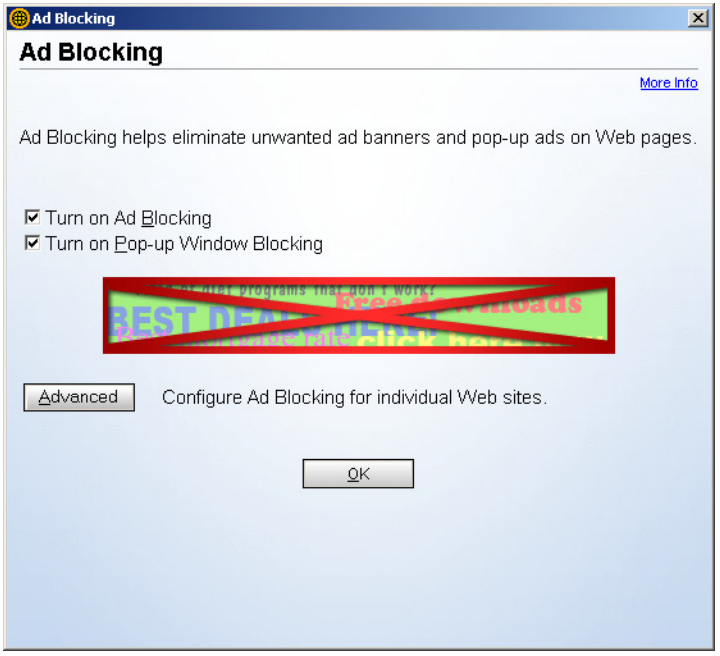
Symantec Client Firewall searches for the addresses of the ads that are being blocked as the Web page is downloaded by your browser. If it finds an address that matches the list of ads to block, it removes the ad so that it does not appear in your browser. It leaves the rest of the Web page intact so that you can view the page without the advertisements.

See "Using advanced Web Content settings" on page 176.

To enable or disable Ad Blocking

1 In the main window, click **Status & Settings**.

2 Double-click **Ad Blocking**.



3 In the Ad Blocking window, do one of the following:

- To enable Ad Blocking, check **Turn on Ad Blocking**.
- To disable Ad Blocking, uncheck **Turn on Ad Blocking**.

4 Click **OK**.

Enabling and disabling Pop-up Window Blocking

Pop-up and pop-under ads are secondary windows that Web sites open when you visit or leave the sites. Pop-ups appear on top of the current window, while pop-unders appear behind the current window.

When Pop-up Window Blocking is active, Symantec Client Firewall automatically blocks the programming code that Web sites use to open secondary windows without your knowledge. Sites that open secondary windows when you click a link or perform other actions are not affected.

Note: Certain Web sites open up a new window when you attempt to download files. Pop-up Window Blocking might block the file download window from appearing. If you attempt to download files and nothing appears to be happening, disable Pop-up Window Blocking temporarily until the file download is completed.

To enable or disable Pop-up Window Blocking

1. In the main window, click **Status & Settings**.
2. Double-click **Ad Blocking**.
3. In the Ad Blocking window, do one of the following:
   - To enable Pop-up Window Blocking, check **Turn on Pop-up Window Blocking**.
   - To disable Pop-up Window Blocking, uncheck **Turn on Pop-up Window Blocking**.
4. Click **OK**.

Using advanced Web Content settings

Web Content settings let you control how Symantec Client Firewall handles interactive online content, ads, and possible privacy intrusions. Web Content settings are arranged on the following three tabs:

- Global Settings
  Lets you control the default and individual Web site actions that Symantec Client Firewall takes when Web sites attempt to get information about your browser or visited sites, or use animated images, scripts, Macromedia Flash, and other active content

- User Settings
  Lets you customize Cookie Blocking, Pop-up Window Blocking, and ActiveX and Java applets for individual Web sites
- Ad Blocking
  Lets you specify individual strings that you want to block for all Web sites. Also, you can specify individual strings that you want to block or allow on individual Web sites

Note: All Web Content filtering is performed on ports that are specified in the HTTP Port List on the Firewall tab in the Symantec Client Firewall Options window. If this list is blank, the firewall does not enforce Web Content settings. Furthermore, Web Content settings are ignored for computers placed in Trusted Zones.

Configuring Global Settings

Global Settings let you control the default and individual Web site actions that Symantec Client Firewall takes when Web sites attempt to get information about your browser or use animated images, scripts, and other active content.

Table 9-2 describes the Global Settings.

Table 9-2 Global Settings

Setting	Description
Information about your browser	Block or allow Web sites to get information about your computer and Web browser.
Information about visited sites	Determine the action that Symantec Client Firewall takes when Web sites request information about other Web sites that you have visited during the current online session. ■ Block ■ Permit same site (default) Requests for information are allowed when the requests originate from the same domain. All other requests are blocked. ■ Permit
Animated images	Block or allow animated images to run. The image still appears but does not animate.
Scripts	Block or allow scripts.
Flash animation	Block or allow animations and ads made with Macromedia Flash.

If the Privacy Control setting is disabled in the Privacy Control window, the Global Settings for Information about your browser and Information about visited sites are ignored.

Enabling and disabling Global Settings

The Global Settings dialog box lets you set default settings for all sites, and allows you to set specific permit or block settings for individual sites.

Some Web sites use Flash to create navigation toolbars. Blocking Flash may make these sites unusable.

To enable or disable Global Settings

1. In the main window, click **Status & Settings**.
2. Double-click one of the following:
   - Privacy Control
   - Ad Blocking
3. In the Privacy Control or Ad Blocking window, click **Advanced**.
4. In the Advanced window, do one of the following:
   - To change default settings for all sites, on the Web Contents Options tab, click **(Defaults)**.
   - To override default settings for a single site, on the Web Contents Options tab, select the name of the site, and then on the Global Settings tab, uncheck **Use Default settings** under one or more settings.
5. For each setting that you want to change, select one of the following:
   - Permit
   - Block
6. Click **OK**.
7. In the Privacy Control or Ad Blocking window, click **OK**.

Configuring User Settings

User Settings let you customize Cookie Blocking, Pop-up Window Blocking, and ActiveX and Java applet settings for individual sites. These settings override default settings that appear in other dialog boxes.

Table 9-3 describes the settings and identifies the dialog boxes that contain the default settings.

Table 9-3 User Settings

Setting	Description	Dialog box
Cookies	Block or allow Web sites to create and read cookie files on your computer	Privacy Control, Customize Privacy Settings
Java Applets	Block or allow Java applets to run	Client Firewall, Customize Security Settings
ActiveX Controls	Block or allow ActiveX controls to run	Client Firewall, Customize Security Settings
Pop-up Ads	Block or allow pop-up ads	Ad Blocking

Two types of cookies exist, persistent and non-persistent. Symantec Client Firewall treats both types the same way.

To configure User Settings

1. In the main window, click **Status & Settings**.
2. Double-click one of the following:
   - Privacy Control
   - Ad Blocking
3. In the Privacy Control or Ad Blocking window, click **Advanced**.
4. In the Advanced window, on the Web Contents Options tab, select a site name.
5. On the User Settings tab, under one or more settings, uncheck the default setting.
6. For each setting that you unchecked, select one of the following:
   - Permit
   - Block
7. Click **OK**.
8. In the Privacy Control or Ad Blocking window, click **OK**.

Configuring Ad Blocking settings

Ad Blocking settings let you specify individual ad banners or groups of ad images that you want to block or allow on individual sites. Symantec Client Firewall detects and blocks ads based on three criteria: their dimensions, locations, and strings.

Note: If you exported a policy file to Symantec Client Firewall with Symantec Client Firewall Administrator, and if the Banner Blocking Client Setting is disabled, Ad Blocking is disabled on Symantec Client Firewall.

About creating text strings that identify ads to block or permit

You can control whether Symantec Client Firewall displays specific ads by creating a list of text strings that identify individual ad banners. Ad Blocking strings are sections of HTML addresses. If any part of a file's address matches the text string, Symantec Client Firewall automatically blocks the file. Symantec Client Firewall provides an Ad Blocking list called (Defaults) that is used to determine which images should be blocked when your browser displays Web pages.

When Ad Blocking is enabled, all Web pages are scanned for the HTML strings specified in the (Defaults) list. Symantec Client Firewall looks for the blocked strings within HTML tags that are used to present advertising. The HTML structures that contain matching strings are removed from the page by Symantec Client Firewall before the page appears in the Web browser.

Make sure that the strings that you place in the (Defaults) block list are not too general. For example, www by itself is not a good string to block because almost every URL includes www. A string like www.slowads is more effective because it only blocks graphics from the slowads domain without affecting other sites.

The way that you define Ad Blocking strings affects how restrictive or unrestrictive Symantec Client Firewall is when filtering data. For example, if you add the string spammersRus.com to the (Defaults) block list, you block everything in the spammersRus.com domain. If you are more specific and add the string /images/image7.gif to the site-specific block list maintained for www.spammersRus.com, you block only that particular image.

You can also create permit strings that allow Web sites to display images that match the string. This allows you to override the blocking effect of any string in the (Defaults) block list for individual sites. Permit rules take precedence over Block rules on any site.

Note: All functionality for adding, modifying, and removing strings is available by right-clicking a string, including the additional functionality of sorting.

Adding an Ad Blocking string

You can add strings to the Ad Blocking list for all sites or for individual sites. Ad Blocking supports lowercase characters only.

To add an Ad Blocking string

1. In the main window, click **Status & Settings**.
2. Double-click one of the following:
   - Privacy Control
   - Ad Blocking
3. In the Privacy Control or Ad Blocking window, click **Advanced**.
4. In the Advanced window, on the Ad Blocking tab, do one of the following:
   - To block a string on all Web sites, on the Web Contents Options tab, click **(Defaults)**.
   - To permit or block a string on a Web site in the list, go to step 5.
5. On the Web Contents Options tab, select the name of the site, and then on the Ad Blocking tab, click **Add**.
6. In the Add New HTML String dialog box, select the action that you want to take. You have the following options:

Block	Block ads that match this string.
Permit	Allow ads that match this string (for individual Web sites only).

7. Type an HTML string to block or permit.
8. Click **OK**.
9. In the Advanced window, click **OK**.
10. In the Privacy Control or Ad Blocking window, click **OK**.

Modifying and removing an Ad Blocking string

If you later decide that an Ad Blocking string is too restrictive, not broad enough, or not appropriate, you can modify or remove it.

To modify or remove an Ad Blocking string

1. In the main window, click **Status & Settings**.
2. Double-click one of the following:
   - Privacy Control
   - Ad Blocking
3. In the Privacy Control or Ad Blocking window, click **Advanced**.
4. In the Advanced window, on the Ad Blocking tab, do one of the following:
   - To modify or remove a string in the (Defaults) list, on the Web Contents Options tab, click **(Defaults)**.
   - To modify or remove a site-specific string, go to step 5.
5. On the Web Contents Options tab, select the name of the site.
6. On the Ad Blocking tab, in the HTML string list, select the string that you want to modify or remove.
7. Do one of the following:
   - To modify a string, click **Modify**, type your changes, and then click **OK**.
   - To remove a string, click **Remove**, and then click **Yes**.
8. In the Advanced window, click **OK**.
9. In the Privacy Control or Ad Blocking window, click **OK**.

Adding and deleting sites

Symantec Client Firewall lets you add sites to or delete sites from the list of Web sites.

Note: When you add a site to the Web Contents Options list, the site must have a different configuration than the default configuration. If you save the site that you want to add without making any changes, the site is dropped from the configuration list because the default settings match your intended configuration for the Web site.

To add and delete sites

1. In the main window, click **Status & Settings**.
2. Double-click one of the following:
   - Privacy Control
   - Ad Blocking
3. In the Privacy Control or Ad Blocking window, click **Advanced**.
4. In the Advanced window, on the Web Contents Options tab, do one of the following:
   - To add a site, click **Add Site**, type a site or domain name, and then click **OK**.
   - To delete a site, select the name of a site, click **Remove Site**, and then click **Yes**.
5. In the Advanced window, click **OK**.
6. In the Privacy Control or Ad Blocking window, click **OK**.

Chapter 10

Monitoring Symantec Client Firewall

This chapter includes the following topics:

About monitoring Symantec Client Firewall

Symantec Client Firewall maintains records of every incoming and outgoing Internet connection and any actions that the program takes to protect your computer. You should periodically review this information to spot potential security violations.

There are three sources of Symantec Client Firewall information:

- Statistics window: Recent information about firewall and content-blocking activities
- Symantec Client Firewall Statistics window: Detailed information about network activity and actions that Symantec Client Firewall has taken
- Log Viewer: Users' Internet activities and any actions that Symantec Client Firewall has taken

When reviewing logged information, check for the following:

- Recent attacks in the Current Status window
- Many denied access attempts, especially from a single IP address

- Sequences of port numbers from the same IP address, possibly indicating a port scan (attackers trying many ports on your computer, looking for one that they can access)
- Excessive network activity by unknown programs

It is normal to see some denied access attempts on a random basis (not all from the same IP address, and not to a sequence of port numbers). You may also see logged access attempts made due to activity on your own computer such as connecting to an FTP server and sending email.

If you see any of the above patterns, it could be evidence of an attack.

Viewing the Statistics window

The Statistics window provides a snapshot of your computer's network activity since the last time that you started Windows. Use this information to identify ongoing attack attempts and review how your Privacy Control settings affect your protection.

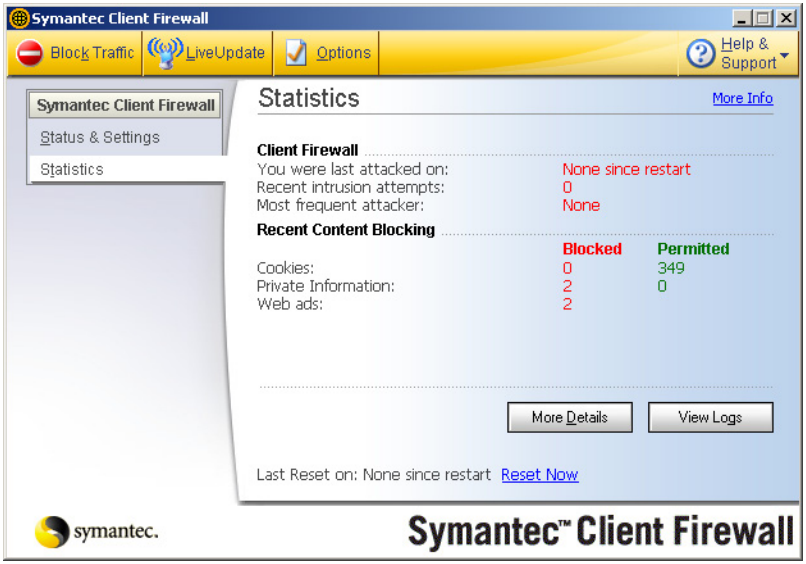
Table 10-1 describes the information that appears in the Statistics window.

Table 10-1 Statistics window information

Section	Information
Client Firewall	Any recent attacks on this computer, including the time of the most recent attack, the frequency of attacks, and the address of the most frequently attacking computer
Recent Content Blocking	The number of times that cookies and private information have been blocked or permitted, and the number of times that Web ads have been blocked

To view the Statistics window

- In the main window, click **Statistics**.



Resetting Statistics window information

Symantec Client Firewall automatically clears all of the statistics in the Statistics window when you restart Windows. You can also clear the statistics manually. This helps you see if a configuration change affects the statistics.

To reset Statistics window information

1. In the main window, click **Statistics**.
2. In the Statistics window, click **Reset Now**.

Viewing the Symantec Client Firewall Statistics window

Along with the overall statistics in the Statistics window, Symantec Client Firewall maintains real-time network counters that track Internet usage and actions that Symantec Client Firewall takes.

Table 10-2 describes the information that appears in the Symantec Client Firewall Statistics window.

Table 10-2 Symantec Client Firewall Statistics window information

Pane	Information
Network	TCP and UDP bytes sent and received, the number of open network connections, and the highest number of simultaneous open network connections since the program started
Online Content	Cookies, private information, and Web ads blocked; and the number of HTTP connections
Firewall TCP Connections	The number of blocked and permitted TCP connections
Firewall UDP Datagrams	The number of blocked and permitted UDP connections
Firewall Rules	All of the rules that are defined for your firewall in the order that they are processed and information about the number of communication attempts that were permitted, blocked, or not matched by firewall rules
Network Connections	Information about current connections, including the program that is using the connection, the protocol being used, and the addresses or names of the connected computers
Last 60 Seconds	The number of network and HTTP connections and the speed of each connection type

To view detailed statistics

1. In the main window, click **Statistics**.
2. In the Statistics window, click **More Details**.

Resetting statistics counters

You can reset the counters to clear all of the statistics and begin accumulating them again. This helps you see if a configuration change affects the statistics.

To reset statistics counters

1. In the main window, click **Statistics**.
2. In the Statistics window, click **More Details**.
3. In the Symantec Client Firewall Statistics window, on the View menu, click **Reset Values**.

Selectively displaying statistics

You can view all detailed statistics at once or display only certain categories.

To selectively display statistics

1. In the main window, click **Statistics**.
2. In the Statistics window, click **More Details**.
3. In the Symantec Client Firewall Statistics window, on the View menu, click **Options**.
4. In the Symantec Client Firewall Statistics Options dialog box, select one or more statistics categories that you want to display.
5. Click **OK**.

Configuring columns

The Symantec Client Firewall Statistics window can display information in one or two columns. Both window layouts display the same statistics.

To configure columns

1. In the main window, click **Statistics**.
2. In the Statistics window, click **More Details**.
3. In the Symantec Client Firewall Statistics window, do one of the following:
   - To automatically adjust between a one-column and two-column display, based on the current window width, on the View menu, click **Columns** > **Automatic**.
   - To always display a single column, on the View menu, click **Columns** > **One**.
   - To always display two columns, on the View menu, click **Columns** > **Two**.

Keeping the Symantec Client Firewall Statistics window visible at all times

You can keep the Symantec Client Firewall Statistics window visible, even when a program runs in a full-screen window. This can be useful for finding unusual network activity that may indicate a security problem.

To keep the Symantec Client Firewall Statistics window visible at all times

1. In the main window, click **Statistics**.
2. In the Statistics window, click **More Details**.
3. In the Symantec Client Firewall Statistics window, on the View menu, click **Always On Top**.

Working with the Log Viewer

Symantec Client Firewall records information about Web sites that you have visited, actions that the firewall has taken, and any alerts that have been triggered. The logs include details about some of the activity reported in the Statistics window.

Table 10-3 describes the tabs that the Log Viewer includes.

Table 10-3 Log Viewer tabs

Tab	Information
Content Blocking	Details about Web ads, Java applets, and ActiveX controls that were blocked by Symantec Client Firewall.
Connections	A history of all TCP/IP network connections made with this computer. Connections are logged when the connection is closed.
Firewall	Traffic intercepted by the firewall, including rules that were processed, alerts displayed, unused ports blocked, and AutoBlock events.
Intrusion Prevention	Whether Intrusion Prevention is active, the attack signatures being monitored, and the number of intrusions that occurred and were blocked.
Privacy	Cookies, computer information, and Web site history information that was blocked or permitted, including the name of the cookie and the Web site that requested the cookie, the name of previous Web sites that were visited, and the name of and details about your computer.
Private Information	Private information sent or blocked.
System	When Symantec Client Firewall has been enabled or disabled, connection activity, and administrator updates to rules, pRules, and IDS settings.
Web History	URLs visited by the computer, providing a history of Web activity.

Table 10-3 Log Viewer tabs

Tab	Information
Alerts	All alert activity, including normal Internet Access Control alerts and security alerts triggered by possible attacks on the Symantec Client Firewall computer.
Configuration	Information regarding configuration changes and updates to rules, Secure Port, and IPS signatures.

About the logging level

Symantec Client Firewall logs information about security attacks, denied connections, and your general computer usage. You can configure rules to create additional log entries when the rules are matched. Certain network traffic that Symantec Client Firewall monitors might not be logged if the logging level is set to Default.

Table 10-4 lists and describes Symantec Client Firewall logging levels.

Table 10-4 Symantec Client Firewall logging levels

Logging level	Description
Default	Provides details about network connections, configuration and system changes, and security alerts, including Intrusion Prevention attacks and Trojan horse attacks. Web sites, private information, and ads that are blocked are also logged.
Verbose	Provides details about all of the events that are logged with the default setting. Logs user agent, information about visited sites, and cookies. Private information, Java applets, ActiveX controls, ads, and Web sites that are allowed are also logged.

Configuring the logging level

You can configure the logging level of Symantec Client Firewall.

To configure the logging level

1. In the main window, click **Options.**
2. Under Logging Level, set the level of logging that you want to use.
3. Click **OK**.

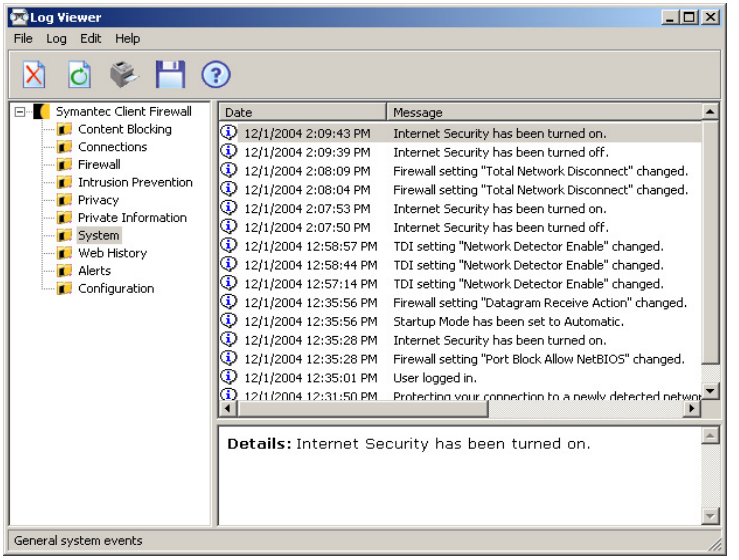
Viewing logs

You can view the Symantec Client Firewall logs from the Statistics window.

To view logs

1 In the main window, click **Statistics**.

2 In the Statistics window, click **View Logs**.



3 In the Log Viewer window, select the log that you want to review.

4 When you are done, select another log or click **File** > **Exit** to close the Log Viewer window.

Refreshing logs

The logs automatically refresh when you move from log to log. To view network events occurring since you began viewing the Log Viewer, you can manually refresh all the logs or an individual log.

Refresh logs

You can refresh all logs and individual logs.

To refresh all logs at once

1. In the main window, click **Statistics**.
2. In the Statistics window, click **View Logs**.
3. In the Log Viewer, right-click **Symantec Client Firewall**, and then click **Refresh all Categories**.

To refresh an individual log

1. In the main window, click **Statistics**.
2. In the Statistics window, click **View Logs**.
3. In the Log Viewer, right-click the log that you want to refresh, and then click **Refresh Category**.

Clearing logs

If you actively use the Internet, or if other computers frequently connect to your computer, the Log Viewer may include information about hundreds of connections. This can make it difficult to identify intruder activity or assess the impact of any changes that you make to Symantec Client Firewall settings.

You can clear Log Viewer tabs to remove logged information. This lets you see how settings changes affect your protection. You can clear a single Log Viewer tab or clear the entire Log Viewer at once.

Clear logs

You can clear events on a single Log Viewer tab or for the entire Log Viewer.

To clear a single log

1. In the main window, click **Statistics**.
2. In the Statistics window, click **View Logs**.
3. In the Log Viewer window, right-click the log that you want to clear, and then click **Clear Category**.

To clear all logs at once

1. In the main window, click **Statistics**.
2. In the Statistics window, click **View Logs**.
3. In the Log Viewer window, right-click **Symantec Client Firewall**, and then click **Clear all Categories**.

Changing the size of the Log Viewer

The Log Viewer stores the information for each tab in a separate file. You can change the size of Log Viewer files to manage the amount of hard disk space that they occupy. When the files reach their maximum size, new events overwrite the oldest events.

By default, all log files are 64 KB. The log file can be increased or decreased by preconfigured increments between 32 KB and 2048 KB. If you want to see information that spans a longer period, increase the size of the log. If you need to recover hard disk space, reduce the size. Changing the size of a log file clears all of the information in that log.

To change the size of the Log Viewer

1. In the main window, click **Statistics**.
2. In the Statistics window, click **View Logs**.
3. In the Log Viewer window, right-click a log, and then click **Change Log File Size**.
4. In the Log File Size dialog box, select a new file size.
5. Click **OK**.

Adjusting column widths in the Log Viewer

You can change the width of the columns in the Log Viewer.

To adjust column widths in the Log Viewer

1. In the main window, click **Statistics**.
2. In the Statistics window, click **View Logs**.
3. In the Log Viewer window, on the tab that you want to view, point to the boundary line on the right side of the column heading.
   The cursor changes from a pointer to a resize tool.
4. Drag the boundary line to the desired width.

Disabling logging

You can select the types of information Symantec Client Firewall tracks in the logs. By default, Symantec Client Firewall tracks events in every category. You can disable individual logs or all logs if you do not need the information that they contain.

Disable logs

You can disable individual logs or all logs.

To disable an individual log

1. In the main window, click **Statistics.**
2. In the Statistics window, click **View Logs.**
3. In the Log Viewer window, right-click the log that you want to disable, and then click **Disable Logging**.

To disable all logs

1. In the main window, click **Statistics**.
2. In the Statistics window, click **View Logs**.
3. In the Log Viewer window, right-click **Symantec Client Firewall,** and then click **Disable All Logging**.

Printing and saving logs and statistics

As you access the Internet, older information in the logs and statistics is overwritten with newer data. To preserve older Internet usage information, or to export this information in word-processing or other documents, print or save the Log Viewer logs and statistics.

Print and save logs and statistics

You can print and save logs and statistics.

To print log information

1. In the main window, click **Statistics**.
2. In the Statistics window, click **View Logs**.
3. In the Log Viewer window, right-click the log that you want to print, and then click **Print Category**.

To print statistics information

1. In the main window, click **Statistics**.
2. In the Statistics window, click **More Details**.
3. In the Symantec Client Firewall Statistics window, on the File menu, click **Print**.
4. In the Print window, click **Print**.

To save log information in a text file

1. In the main window, click **Statistics**.
2. In the Statistics window, click **View Logs**.
3. In the Log Viewer window, right-click the log that you want to save, and then click **Export Category As**.
4. Specify a location and name for the text file.
5. Click **Save**.

To save statistics to a text file

1. In the main window, click **Statistics**.
2. In the Statistics window, click **More Details**.
3. In the Symantec Client Firewall Statistics window, on the File menu, click **Save**.
4. Specify a location and name for the text file.
5. Click **Save**.

Index

J

L

M

N

O

P

Q

R

S

T

U

V

W

Z